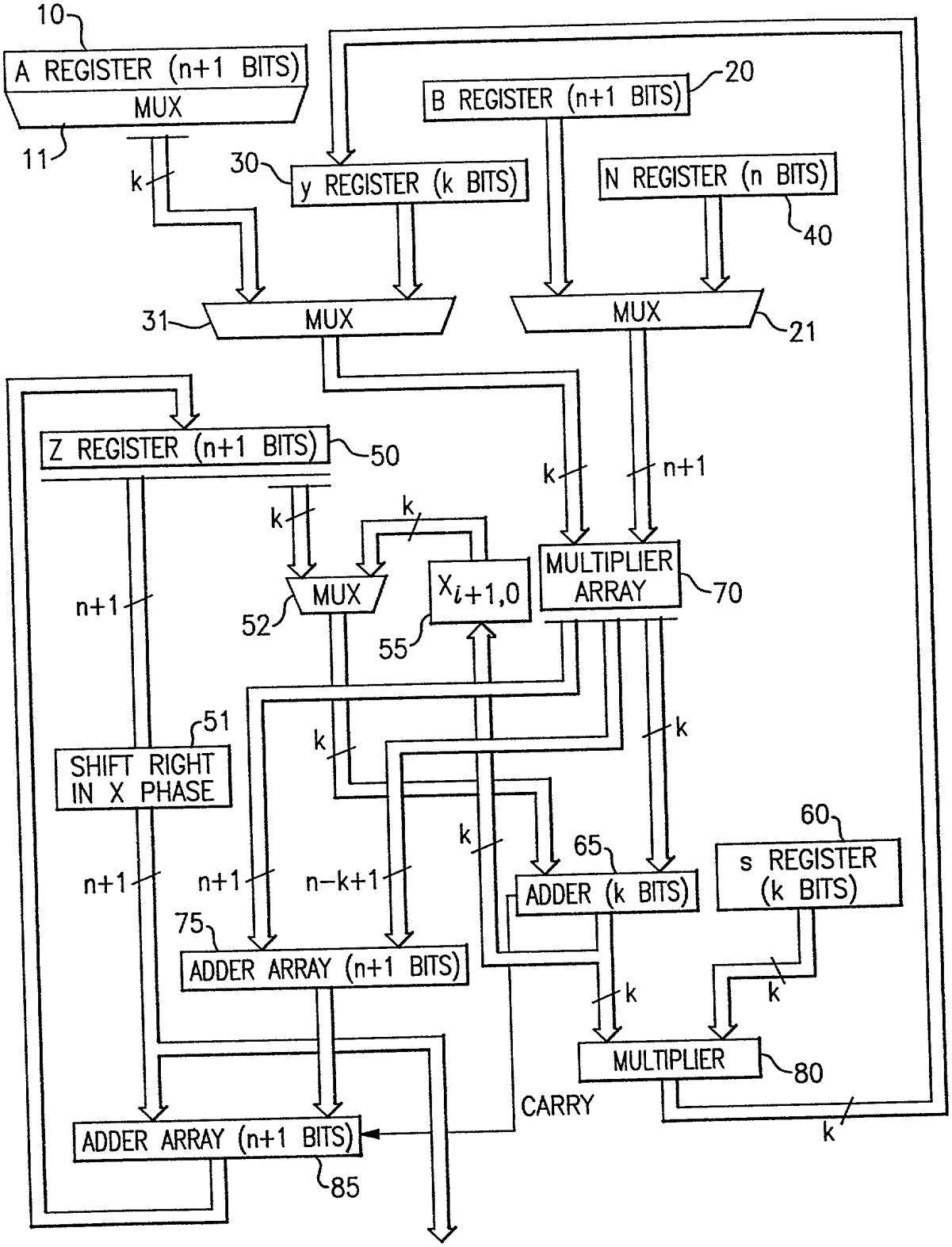
10
A REGISTER (n+1 BITS)
MUX
11
B REGISTER (n+1 BITS)
20
30
y REGISTER (k BITS)
N REGISTER (n BITS)
40
k
31
MUX
MUX
21
Z REGISTER (n+1 BITS)
50
k
n+1
k
k
n+1
MUX
52
$X_{i+1,0}$
55
MULTIPLIER ARRAY
70
51
SHIFT RIGHT IN X PHASE
k
k
60
k
65
s REGISTER (k BITS)
n+1
n+1
n−k+1
ADDER (k BITS)
75
ADDER ARRAY (n+1 BITS)
k
k
MULTIPLIER
80
CARRY
ADDER ARRAY (n+1 BITS)
85
k

FIG.1

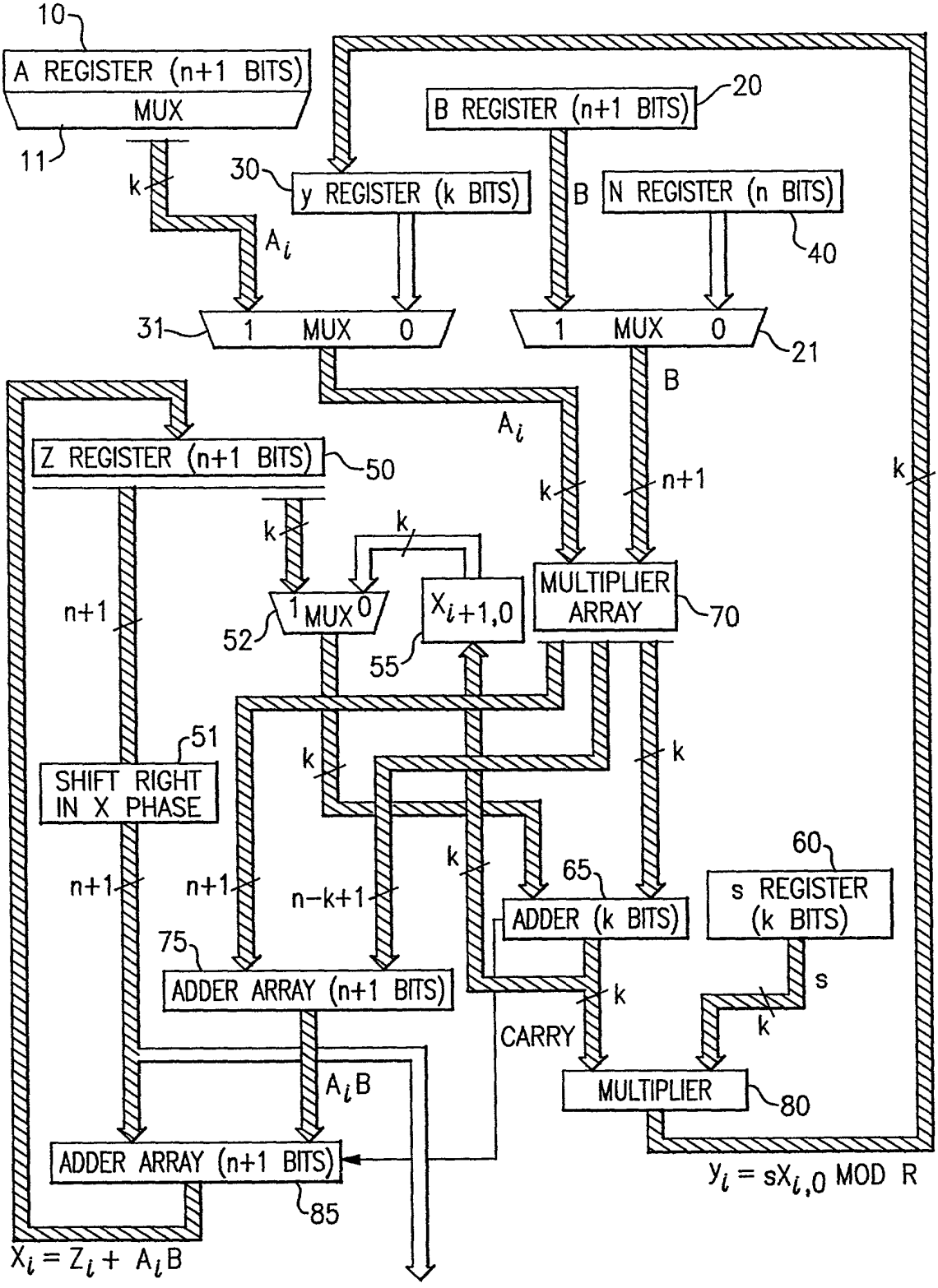
10
A REGISTER (n+1 BITS)
MUX
11
k
A_i
30
y REGISTER (k BITS)
B REGISTER (n+1 BITS)
20
B
N REGISTER (n BITS)
40
31
1 MUX 0
1 MUX 0
21
B
A_i
Z REGISTER (n+1 BITS)
50
k
n+1
k
k
k
n+1
1 MUX 0
52
$X_{i+1,0}$
55
MULTIPLIER ARRAY
70
51
SHIFT RIGHT IN X PHASE
k
k
60
k
65
n+1
n+1
n−k+1
ADDER (k BITS)
s REGISTER (k BITS)
75
ADDER ARRAY (n+1 BITS)
k
s
k
CARRY
A_iB
MULTIPLIER
80
ADDER ARRAY (n+1 BITS)
85
$y_i = sX_{i,0}$ MOD R
$X_i = Z_i + A_iB$

FIG.2

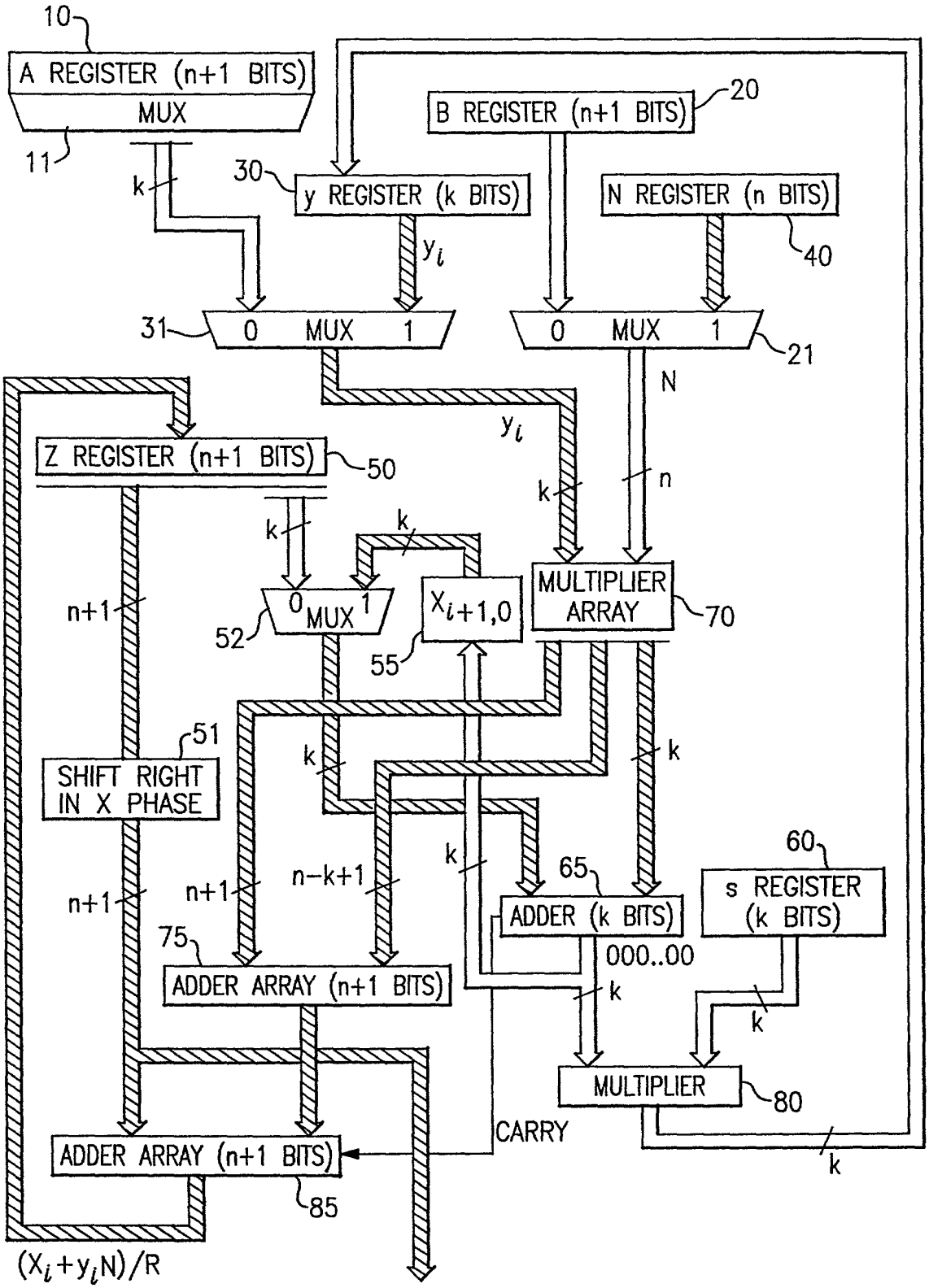
10
A REGISTER (n+1 BITS)
MUX
11
B REGISTER (n+1 BITS)
20
30
y REGISTER (k BITS)
N REGISTER (n BITS)
40
k
y_i
31
0 MUX 1
0 MUX 1
21
N
y_i
Z REGISTER (n+1 BITS)
50
k
n
k
k
n+1
0 MUX 1
52
$X_{i+1,0}$
55
MULTIPLIER ARRAY
70
51
SHIFT RIGHT IN X PHASE
k
k
60
n+1
n+1
n−k+1
k
65
s REGISTER (k BITS)
ADDER (k BITS)
75
000..00
ADDER ARRAY (n+1 BITS)
k
k
MULTIPLIER
80
CARRY
ADDER ARRAY (n+1 BITS)
85
k
$(X_i+y_iN)/R$

FIG.3

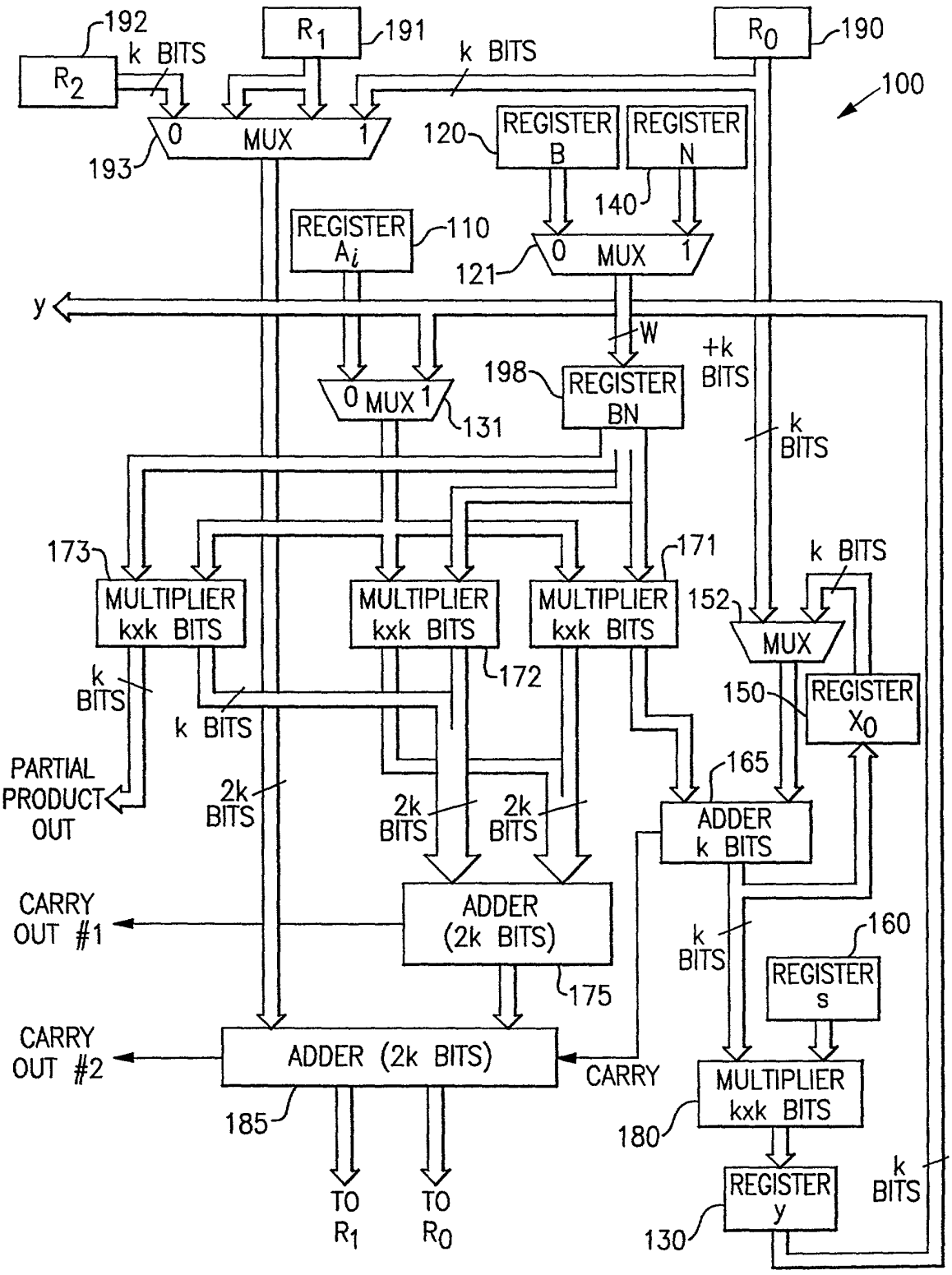
192
k BITS
R2
R1
191
k BITS
R0
190
100
0 MUX 1
193
120
REGISTER B
REGISTER N
140
REGISTER Ai
110
0 MUX 1
121
y
W
+k BITS
198
REGISTER BN
0 MUX 1
131
k BITS
173
171
k BITS
MULTIPLIER kxk BITS
MULTIPLIER kxk BITS
MULTIPLIER kxk BITS
152
MUX
k BITS
172
150
REGISTER X0
k BITS
k BITS
PARTIAL PRODUCT OUT
2k BITS
2k BITS
2k BITS
165
ADDER k BITS
ADDER (2k BITS)
CARRY OUT #1
k BITS
160
REGISTER s
175
CARRY OUT #2
ADDER (2k BITS)
CARRY
MULTIPLIER kxk BITS
185
180
TO R1
TO R0
REGISTER y
k BITS
130

FIG.4

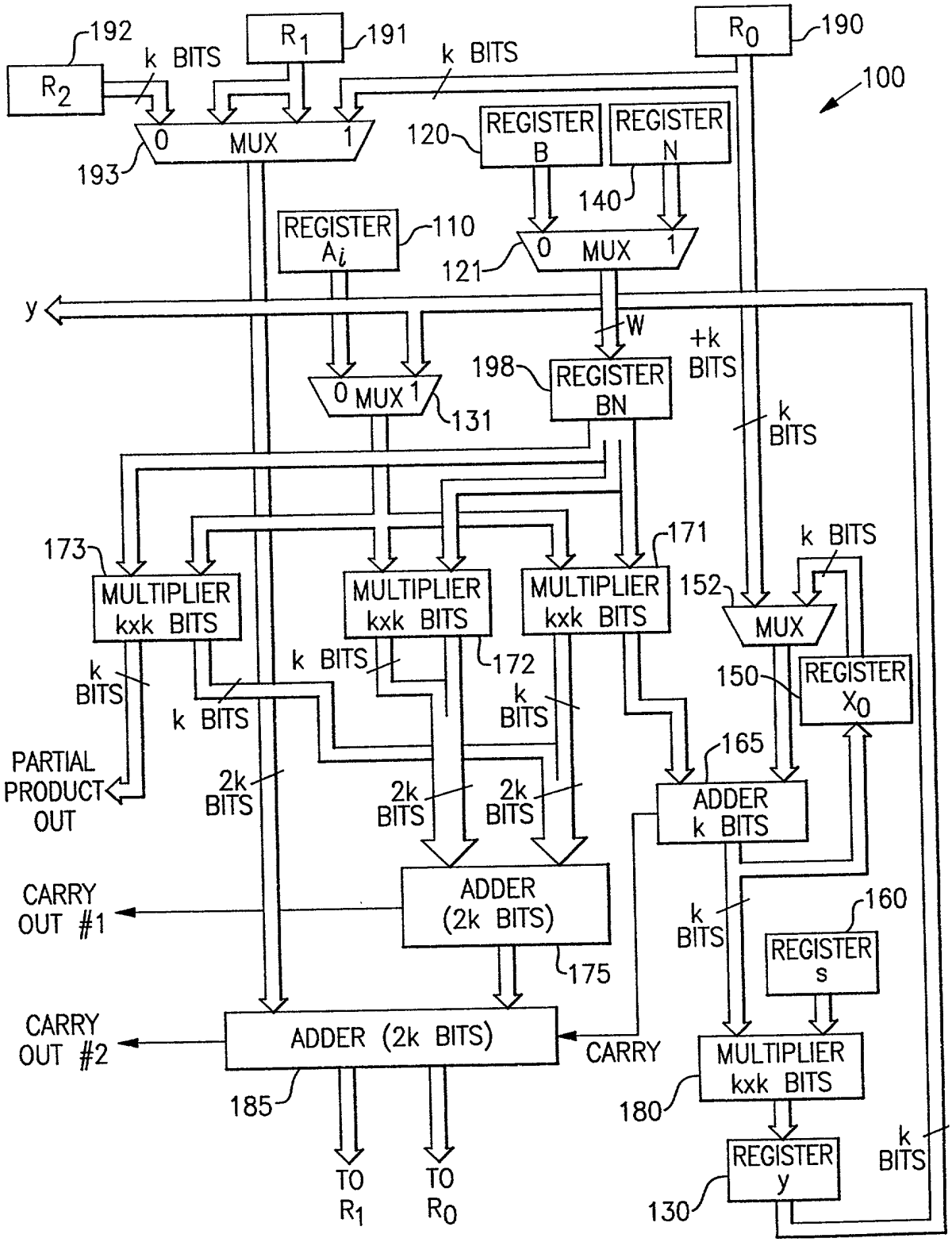
192
k BITS
R1
191
k BITS
R0
190
100
R2
0 MUX 1
193
120
REGISTER B
REGISTER N
140
REGISTER Ai
110
0 MUX 1
121
y
W
+k BITS
198
REGISTER BN
0 MUX 1
131
k BITS
173
171
k BITS
MULTIPLIER kxk BITS
MULTIPLIER kxk BITS
MULTIPLIER kxk BITS
152
MUX
k BITS
k BITS
k BITS
172
k BITS
150
REGISTER X0
PARTIAL PRODUCT OUT
2k BITS
2k BITS
2k BITS
165
ADDER k BITS
ADDER (2k BITS)
CARRY OUT #1
k BITS
160
REGISTER s
175
CARRY OUT #2
ADDER (2k BITS)
CARRY
MULTIPLIER kxk BITS
180
185
REGISTER y
k BITS
130
TO R1
TO R0

FIG.4A

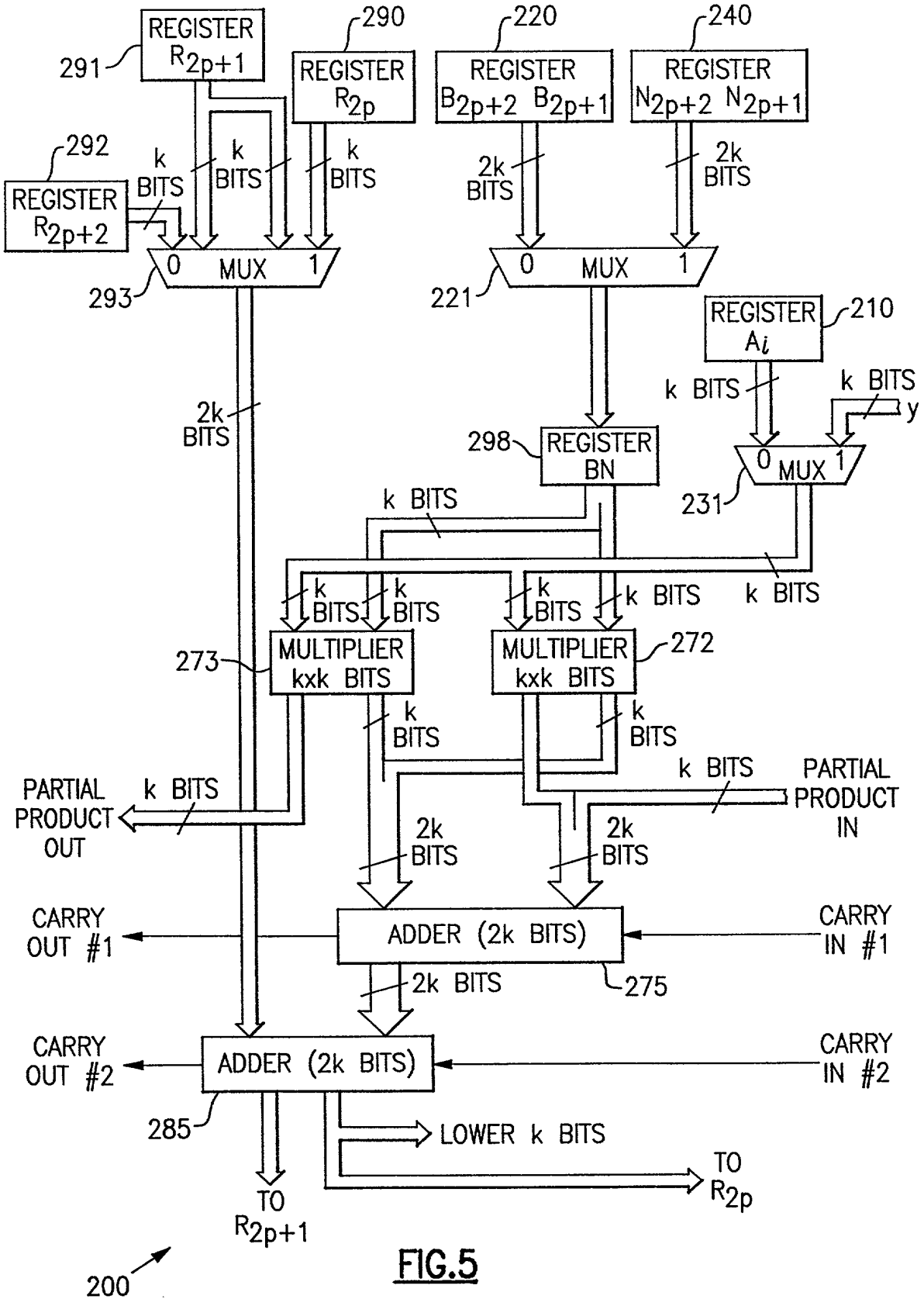
REGISTER R_{2p+1}
291
290
REGISTER R_{2p}
220
REGISTER B_{2p+2} B_{2p+1}
240
REGISTER N_{2p+2} N_{2p+1}
292
REGISTER R_{2p+2}
k BITS
2k BITS
0 MUX 1
293
221
REGISTER A_i
210
y
298
REGISTER BN
231
MULTIPLIER kxk BITS
273
272
PARTIAL PRODUCT OUT
PARTIAL PRODUCT IN
ADDER (2k BITS)
CARRY OUT #1
CARRY IN #1
CARRY OUT #2
CARRY IN #2
285
LOWER k BITS
TO R_{2p}
TO R_{2p+1}
200

FIG.5

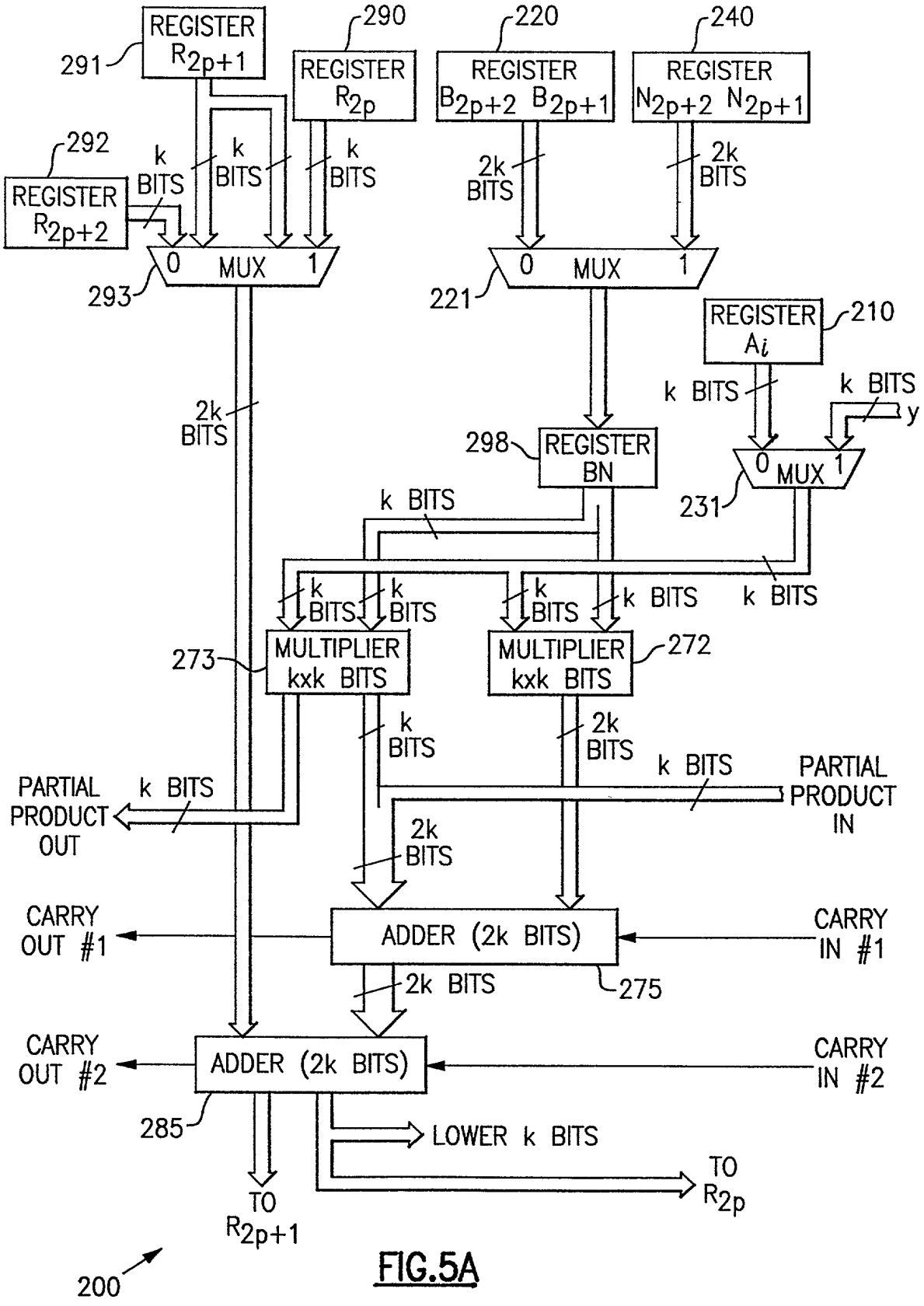
REGISTER R2p+1
291
290
REGISTER R2p
220
REGISTER B2p+2 B2p+1
240
REGISTER N2p+2 N2p+1
292
REGISTER R2p+2
k BITS
k BITS
k BITS
2k BITS
2k BITS
0 MUX 1
293
0 MUX 1
221
REGISTER Ai
210
k BITS
k BITS
y
2k BITS
298
REGISTER BN
0 MUX 1
231
k BITS
k BITS
k BITS
k BITS
k BITS
k BITS
MULTIPLIER kxk BITS
273
MULTIPLIER kxk BITS
272
k BITS
2k BITS
PARTIAL PRODUCT OUT
k BITS
k BITS
PARTIAL PRODUCT IN
2k BITS
CARRY OUT #1
ADDER (2k BITS)
CARRY IN #1
2k BITS
275
CARRY OUT #2
ADDER (2k BITS)
CARRY IN #2
285
LOWER k BITS
TO R2p
TO R2p+1
200

FIG.5A

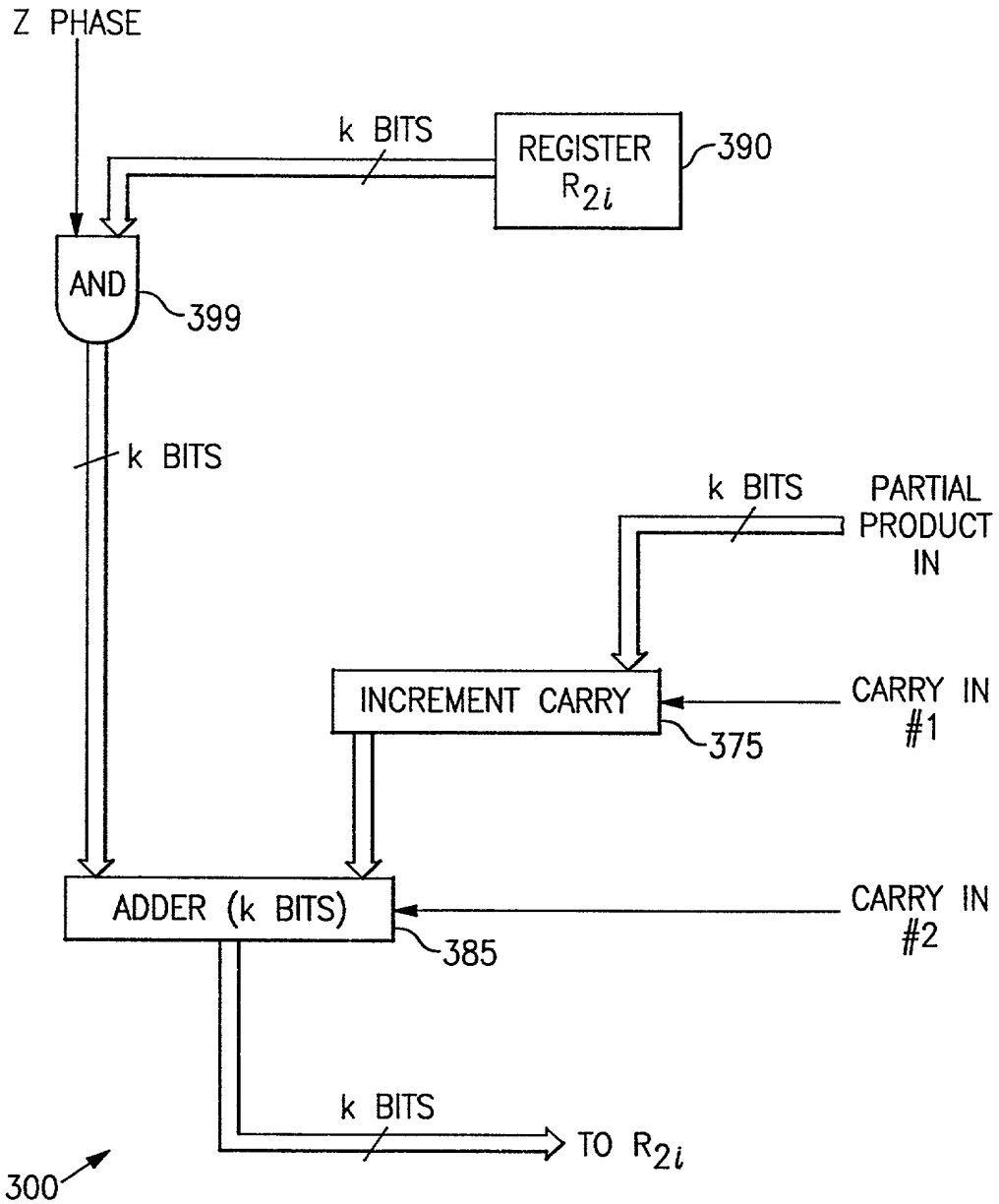
Z PHASE
k BITS
REGISTER
R_{2i}
390
AND
399
k BITS
k BITS
PARTIAL
PRODUCT
IN
INCREMENT CARRY
CARRY IN
#1
375
ADDER (k BITS)
CARRY IN
#2
385
k BITS
TO R_{2i}
300

FIG.6

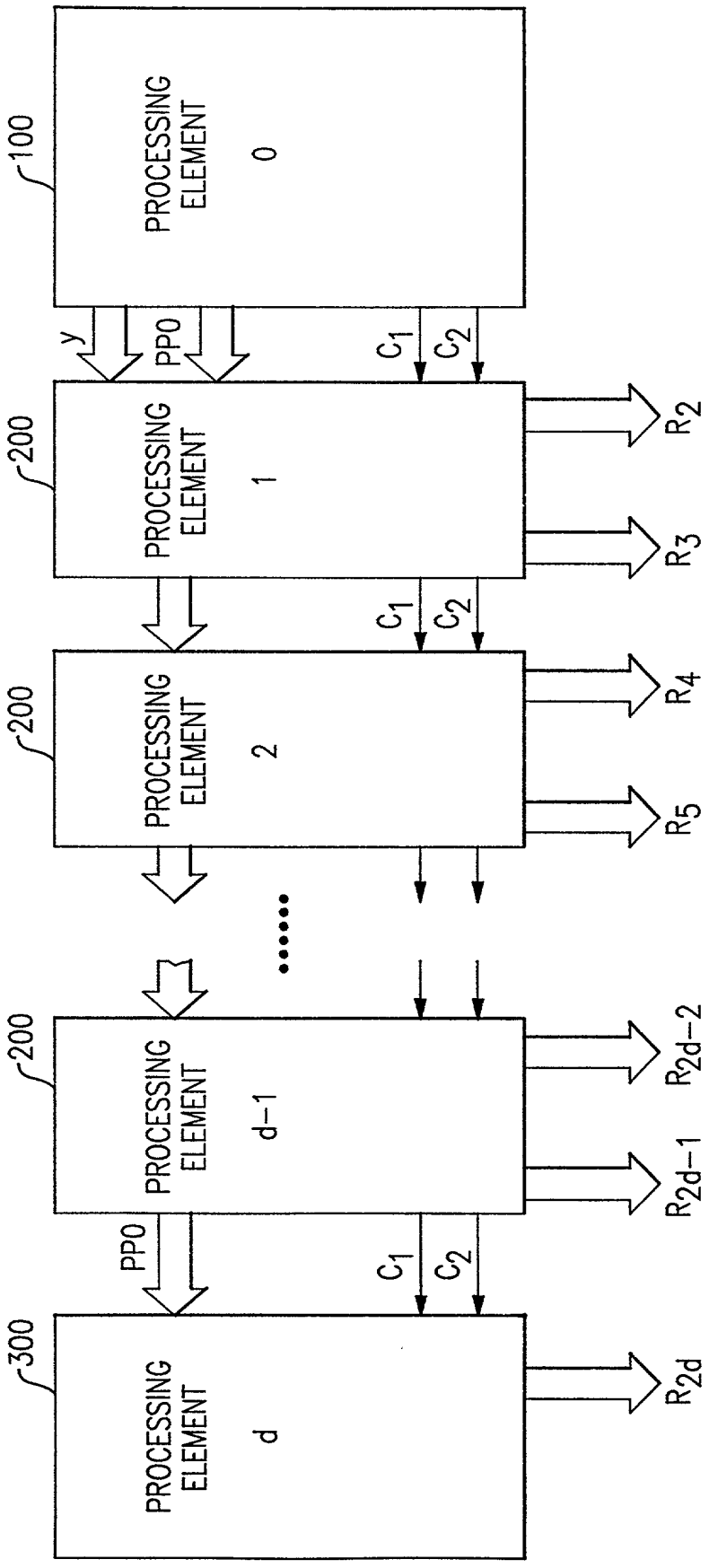
100
PROCESSING ELEMENT 0
y
PP0
C1
C2
200
PROCESSING ELEMENT 1
R2
R3
200
PROCESSING ELEMENT 2
R4
R5
200
PROCESSING ELEMENT d-1
R2d-2
R2d-1
PP0
C1
C2
300
PROCESSING ELEMENT d
R2d

FIG.7

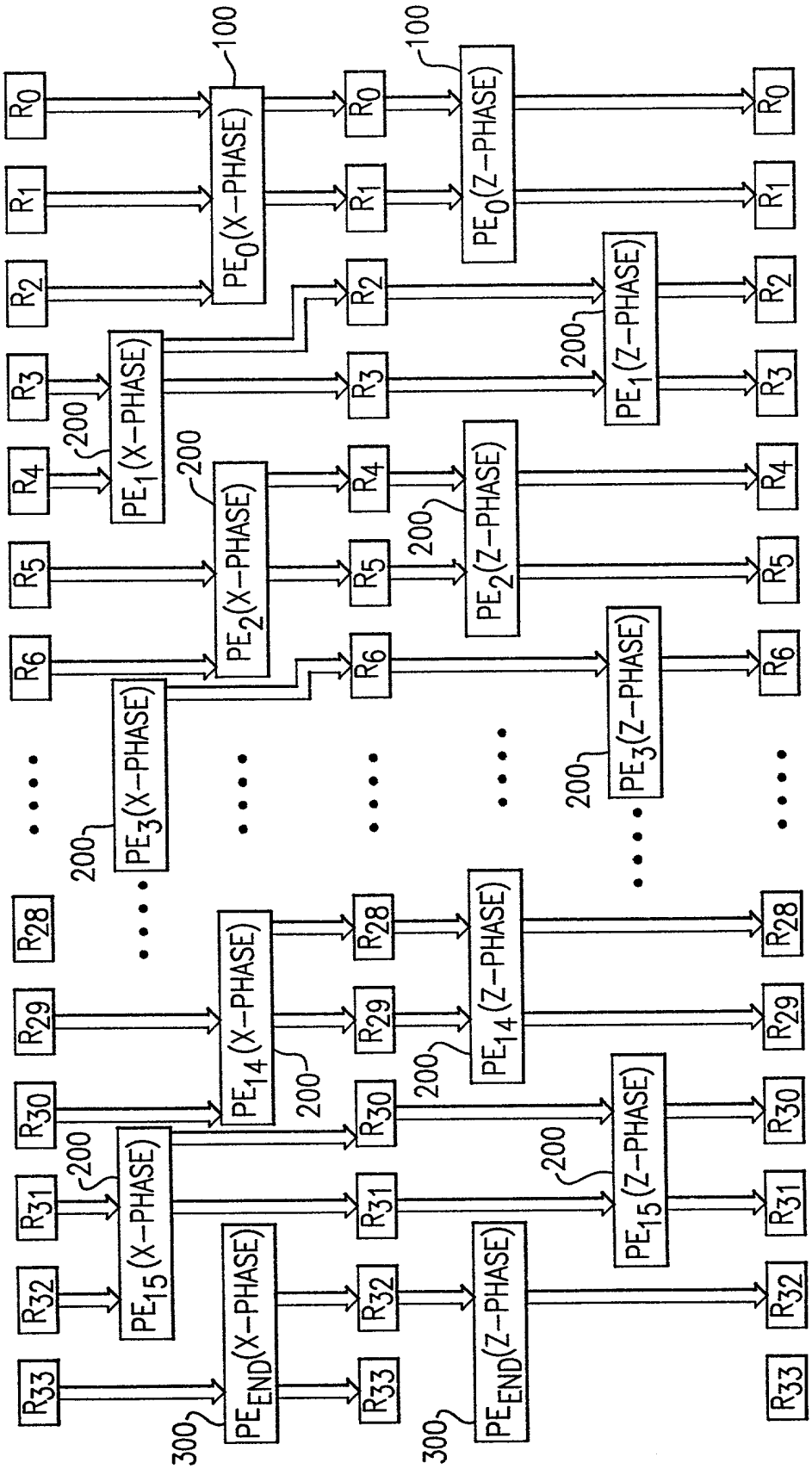
R0
R1
R2
R3
R4
R5
R6
R28
R29
R30
R31
R32
R33
100
PE0(X-PHASE)
PE0(Z-PHASE)
200
PE1(X-PHASE)
PE1(Z-PHASE)
PE2(X-PHASE)
PE2(Z-PHASE)
PE3(X-PHASE)
PE3(Z-PHASE)
PE14(X-PHASE)
PE14(Z-PHASE)
PE15(X-PHASE)
PE15(Z-PHASE)
300
PEEND(X-PHASE)
PEEND(Z-PHASE)

FIG.8

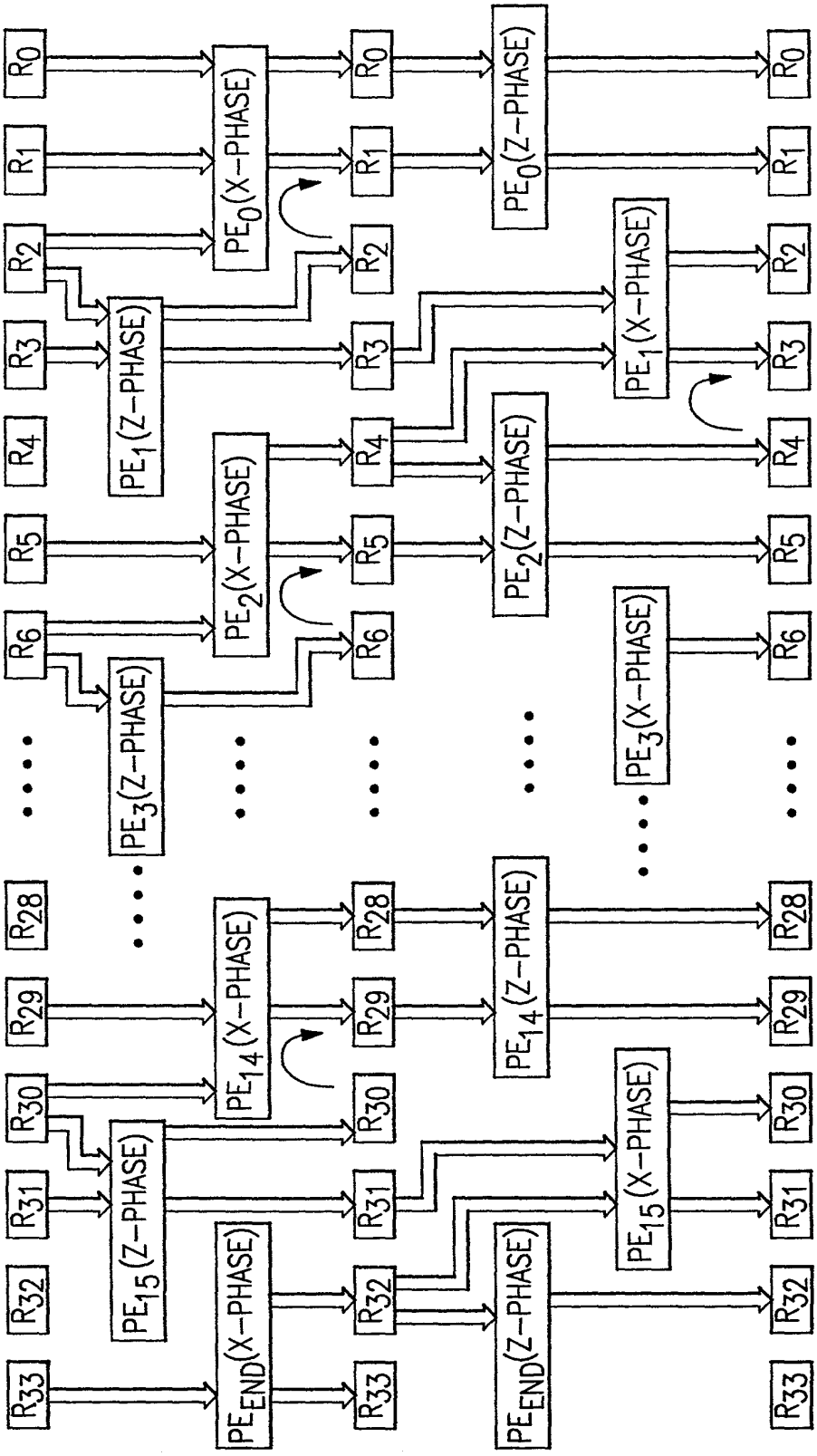
R0
R1
R2
R3
R4
R5
R6
R28
R29
R30
R31
R32
R33
PE0(X-PHASE)
PE1(Z-PHASE)
PE2(X-PHASE)
PE3(Z-PHASE)
PE14(X-PHASE)
PE15(Z-PHASE)
PEEND(X-PHASE)
PE0(Z-PHASE)
PE1(X-PHASE)
PE2(Z-PHASE)
PE3(X-PHASE)
PE14(Z-PHASE)
PE15(X-PHASE)
PEEND(Z-PHASE)

FIG.9

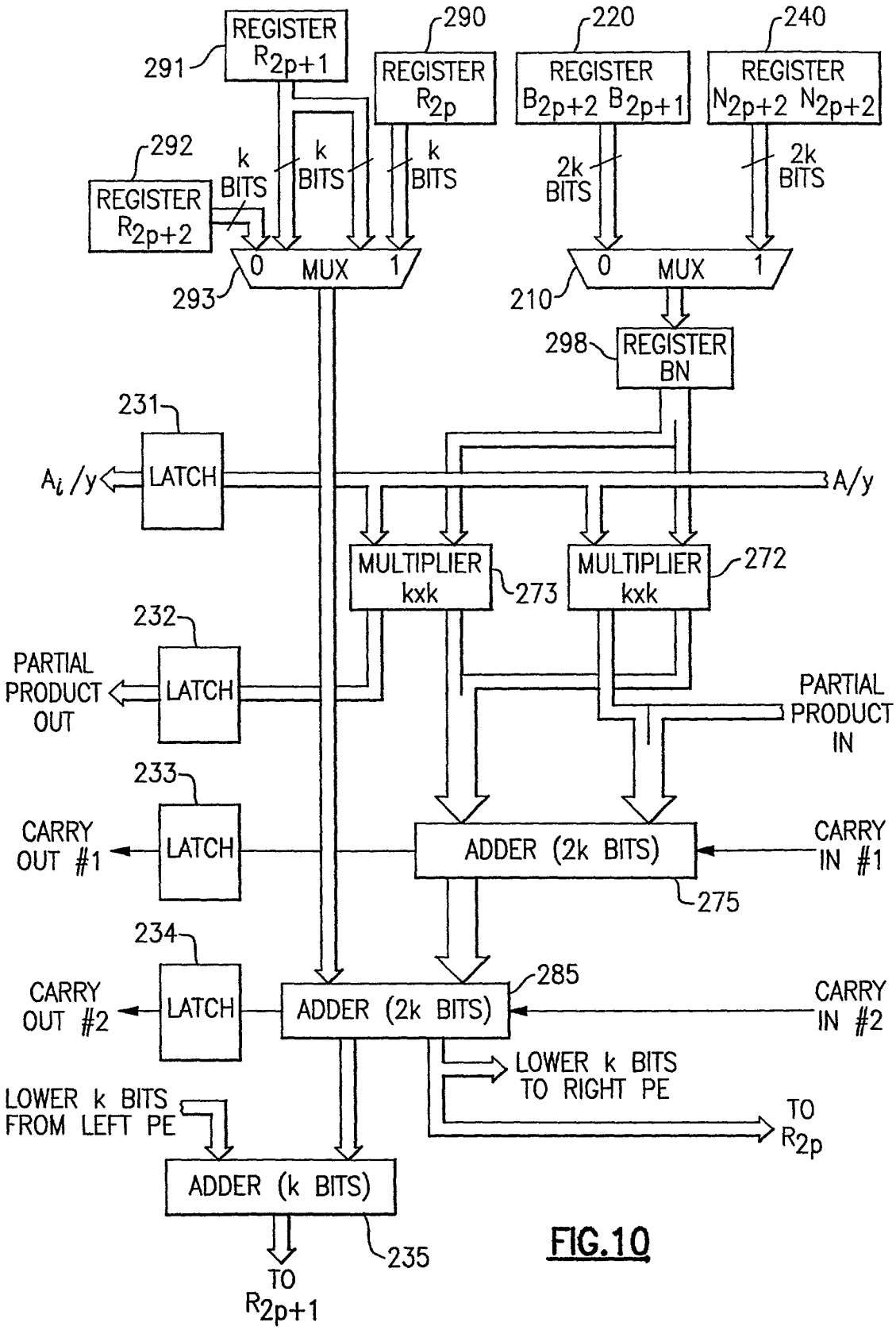
REGISTER R_{2p+1}
291
290
REGISTER R_{2p}
220
REGISTER B_{2p+2} B_{2p+1}
240
REGISTER N_{2p+2} N_{2p+2}
292
REGISTER R_{2p+2}
k BITS
k BITS
k BITS
2k BITS
2k BITS
0 MUX 1
293
0 MUX 1
210
298
REGISTER BN
231
LATCH
A_i /y
A/y
MULTIPLIER kxk
273
MULTIPLIER kxk
272
232
LATCH
PARTIAL PRODUCT OUT
PARTIAL PRODUCT IN
233
LATCH
CARRY OUT #1
ADDER (2k BITS)
CARRY IN #1
275
234
LATCH
CARRY OUT #2
ADDER (2k BITS)
285
CARRY IN #2
LOWER k BITS TO RIGHT PE
TO R_{2p}
LOWER k BITS FROM LEFT PE
ADDER (k BITS)
235
TO R_{2p+1}

FIG.10

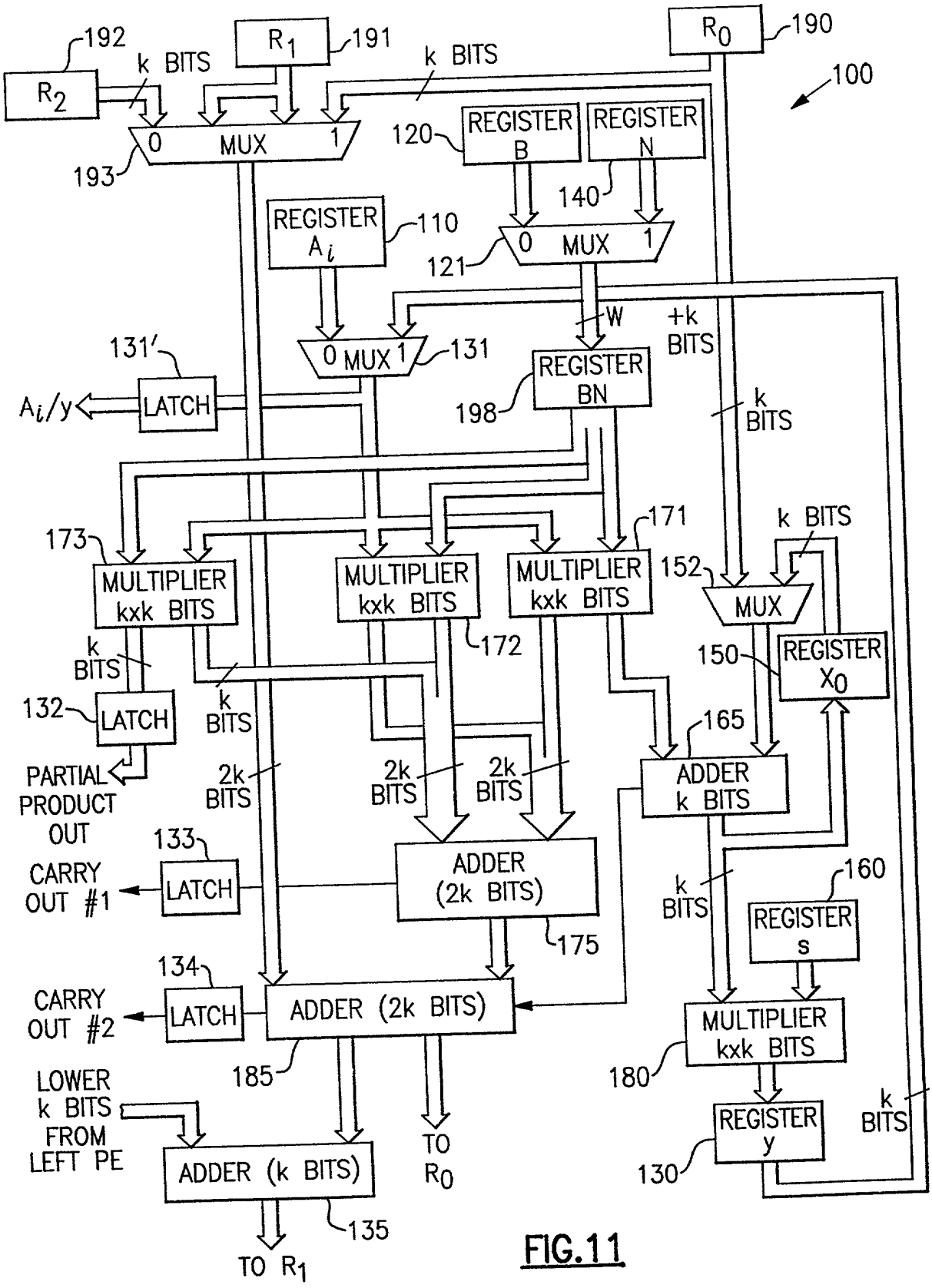
R2
192
k BITS
R1
191
k BITS
R0
190
100
0 MUX 1
193
120
REGISTER B
REGISTER N
140
REGISTER Ai
110
0 MUX 1
121
W
+k BITS
131'
0 MUX 1
131
LATCH
Ai/y
REGISTER BN
198
k BITS
173
MULTIPLIER kxk BITS
MULTIPLIER kxk BITS
MULTIPLIER kxk BITS
171
k BITS
152
MUX
k BITS
172
150
REGISTER X0
132
LATCH
k BITS
PARTIAL PRODUCT OUT
2k BITS
2k BITS
2k BITS
165
ADDER k BITS
133
CARRY OUT #1
LATCH
ADDER (2k BITS)
175
k BITS
160
REGISTER s
134
CARRY OUT #2
LATCH
ADDER (2k BITS)
185
MULTIPLIER kxk BITS
180
LOWER k BITS FROM LEFT PE
ADDER (k BITS)
TO R0
REGISTER y
130
k BITS
135
TO R1

FIG.11

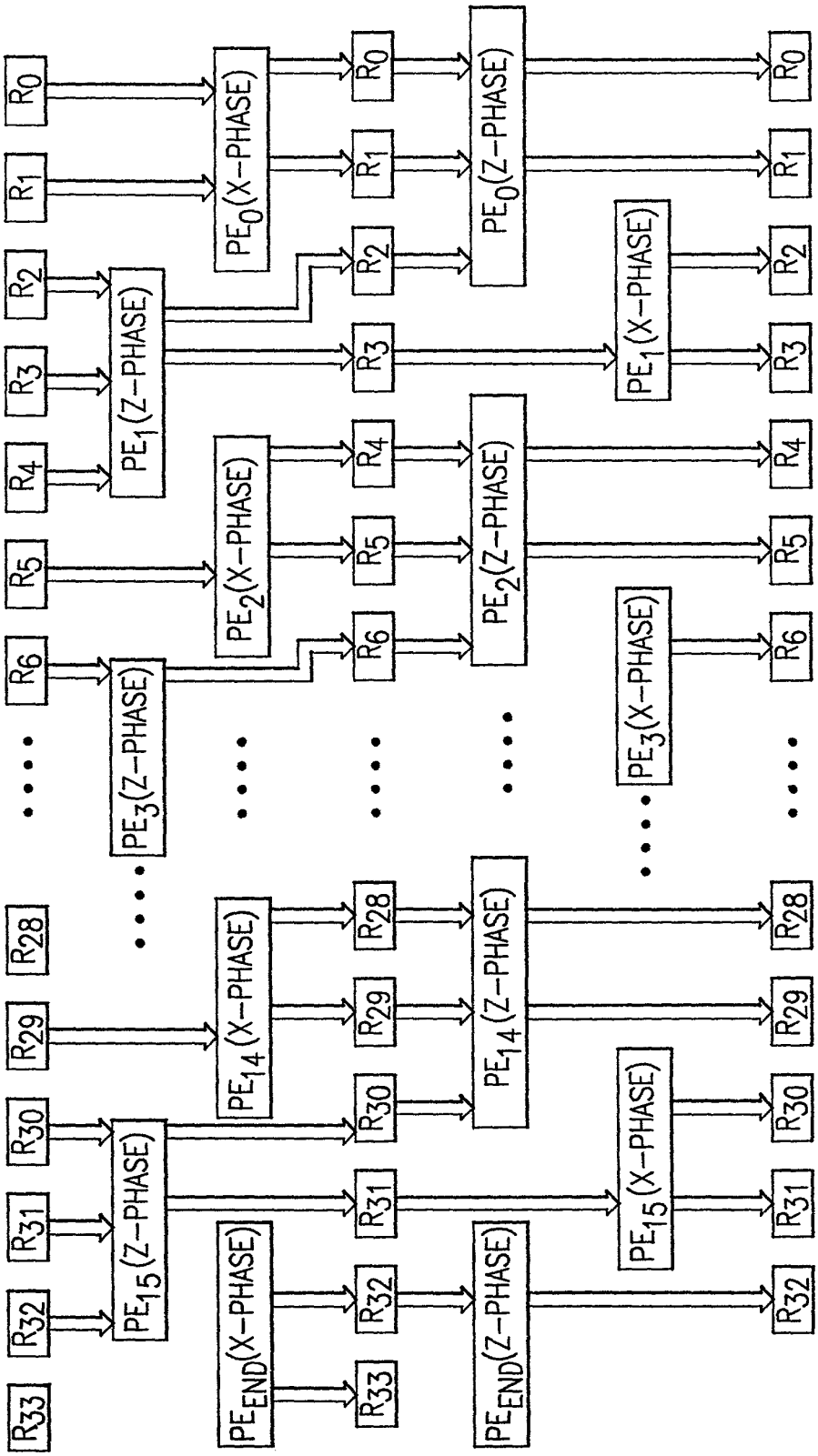
R0
R1
R2
R3
R4
R5
R6
R28
R29
R30
R31
R32
R33
PE0(X-PHASE)
PE0(Z-PHASE)
PE1(Z-PHASE)
PE1(X-PHASE)
PE2(X-PHASE)
PE2(Z-PHASE)
PE3(Z-PHASE)
PE3(X-PHASE)
PE14(X-PHASE)
PE14(Z-PHASE)
PE15(Z-PHASE)
PE15(X-PHASE)
PEEND(X-PHASE)
PEEND(Z-PHASE)

FIG.12

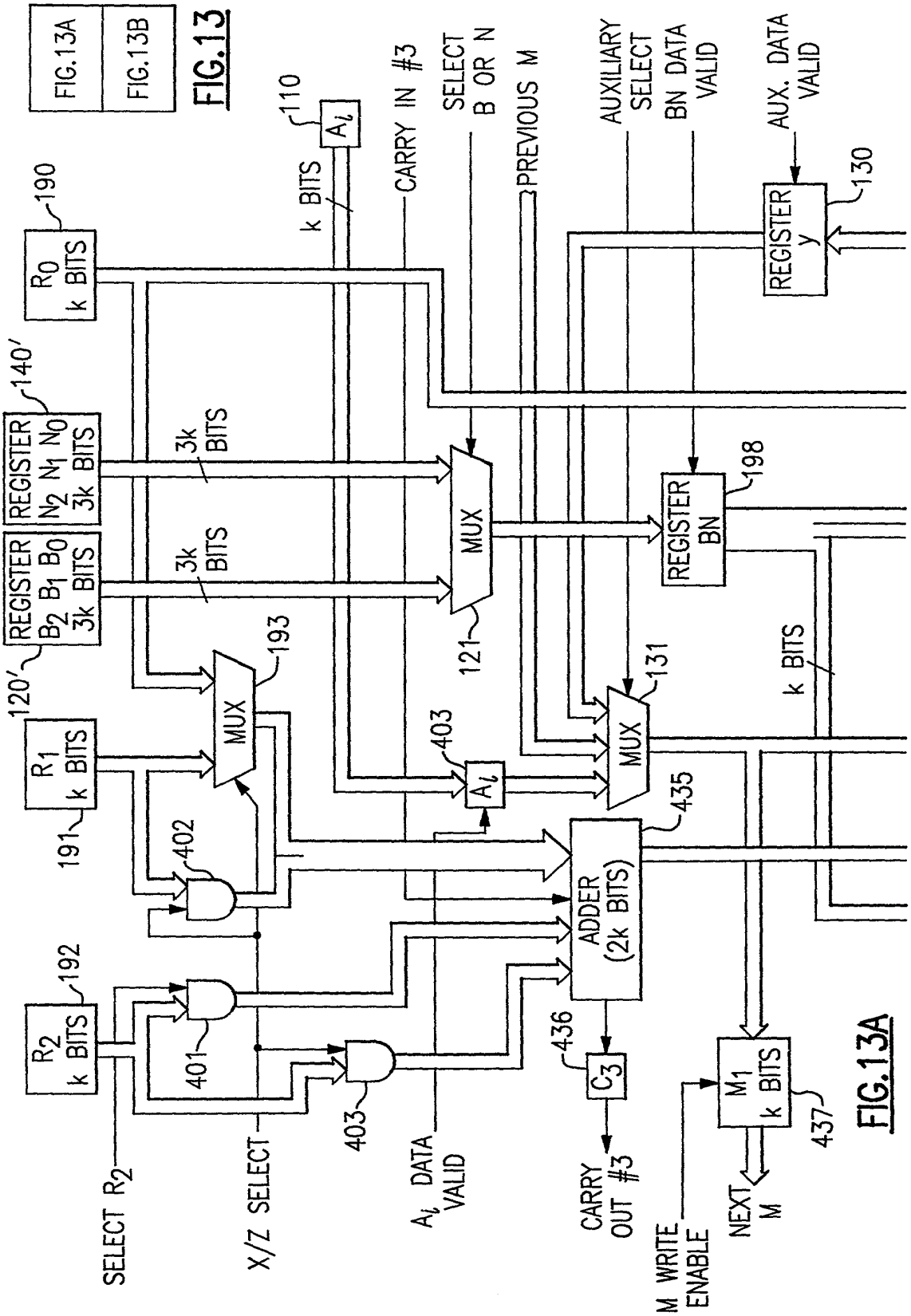
FIG.13A
FIG.13B
FIG.13
110
A_i
k BITS
CARRY IN #3
SELECT B OR N
PREVIOUS M
AUXILIARY SELECT
BN DATA VALID
AUX. DATA VALID
190
R_0 k BITS
140'
REGISTER N_2 N_1 N_0 3k BITS
3k BITS
REGISTER B_2 B_1 B_0 3k BITS
120'
MUX
121
REGISTER y
130
REGISTER BN
198
193
R_1 k BITS
191
402
403
A_i
MUX
131
k BITS
435
ADDER (2k BITS)
R_2 k BITS
192
401
403
436
C_3
M_1 k BITS
437
SELECT R_2
X/Z SELECT
A_i DATA VALID
CARRY OUT #3
M WRITE ENABLE
NEXT M

FIG.13A

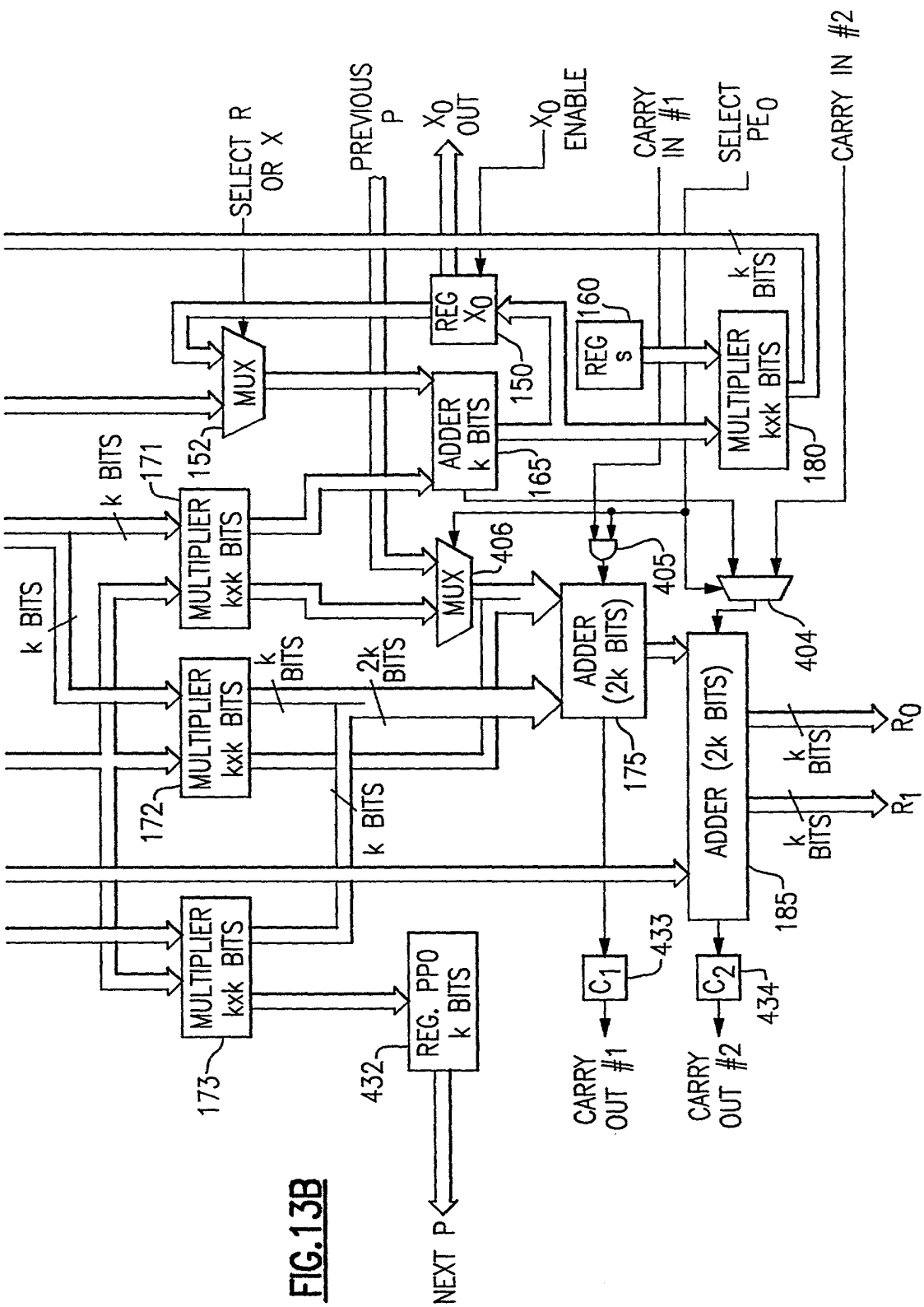
SELECT R OR X
PREVIOUS P
X_0 OUT
X_0 ENABLE
CARRY IN #1
SELECT PE_0
CARRY IN #2
k BITS
MUX
REG X_0
150
REG s
160
ADDER k BITS
165
MULTIPLIER kxk BITS
180
171
152
MULTIPLIER kxk BITS
MUX
406
405
ADDER (2k BITS)
175
404
2k BITS
172
MULTIPLIER kxk BITS
ADDER (2k BITS)
185
R_0
R_1
173
MULTIPLIER kxk BITS
REG. PP0 k BITS
432
C_1
433
C_2
434
CARRY OUT #1
CARRY OUT #2
NEXT P

FIG.13B

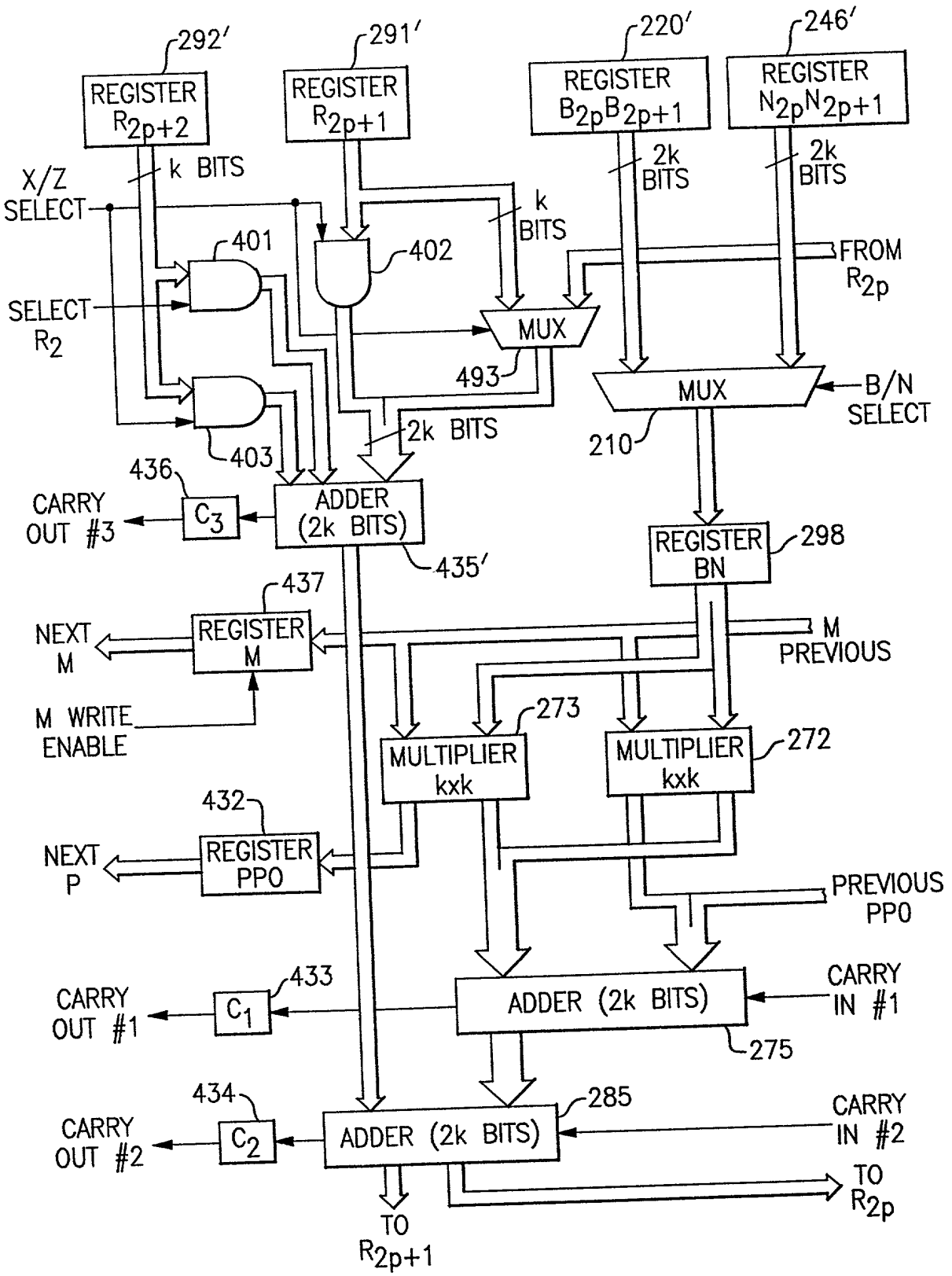
292′
REGISTER R_{2p+2}
291′
REGISTER R_{2p+1}
220′
REGISTER $B_{2p}B_{2p+1}$
246′
REGISTER $N_{2p}N_{2p+1}$
k BITS
2k BITS
2k BITS
X/Z SELECT
k BITS
401
402
FROM R_{2p}
SELECT R_2
MUX
493
MUX
B/N SELECT
210
2k BITS
403
436
CARRY OUT #3
C_3
ADDER (2k BITS)
435′
REGISTER BN
298
437
NEXT M
REGISTER M
M PREVIOUS
M WRITE ENABLE
MULTIPLIER kxk
273
MULTIPLIER kxk
272
432
NEXT P
REGISTER PP0
PREVIOUS PP0
CARRY OUT #1
433
C_1
ADDER (2k BITS)
CARRY IN #1
275
434
CARRY OUT #2
C_2
ADDER (2k BITS)
285
CARRY IN #2
TO R_{2p}
TO R_{2p+1}

FIG.14

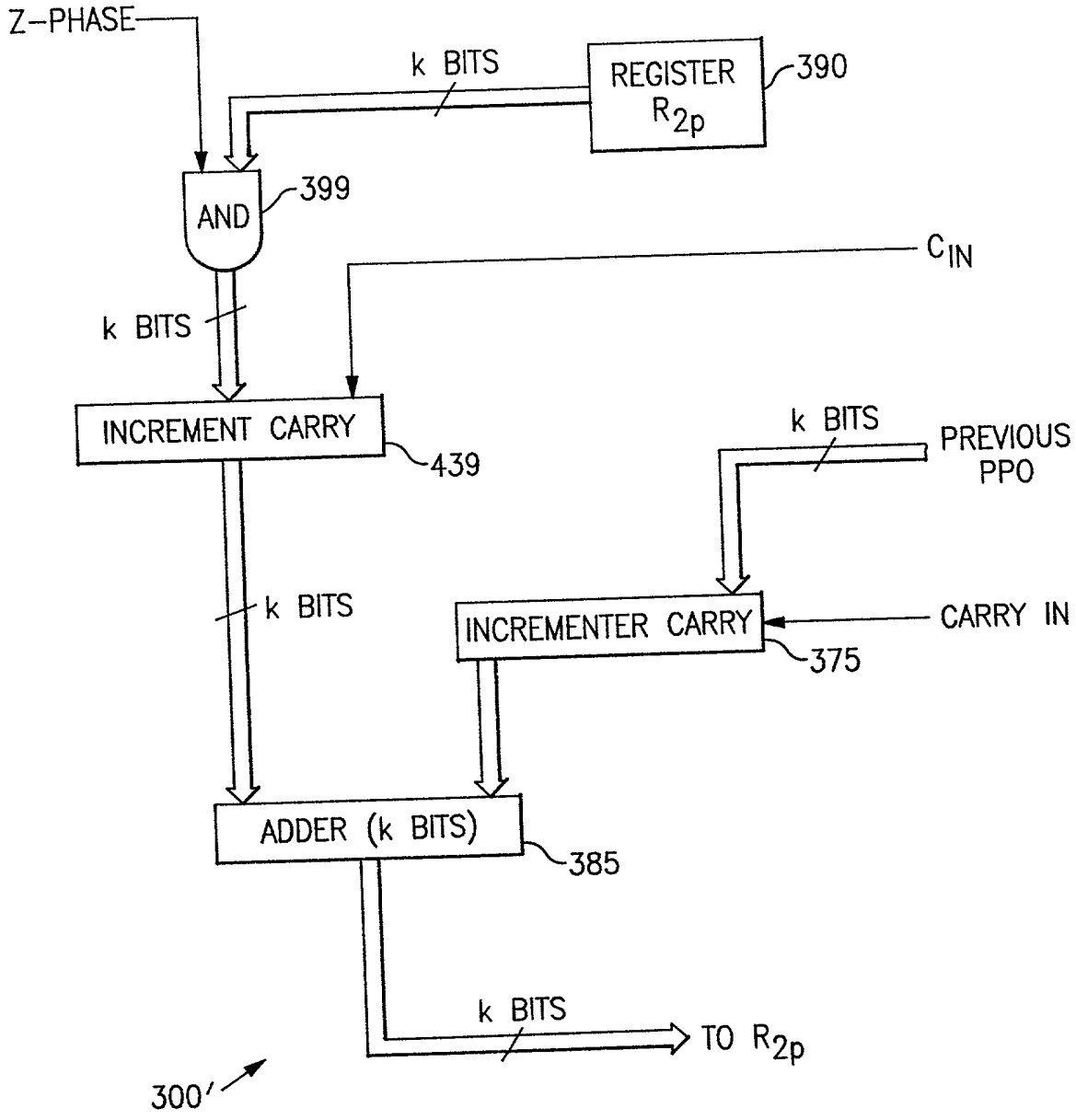
Z-PHASE
k BITS
REGISTER
R_{2p}
390
AND
399
C_{IN}
k BITS
INCREMENT CARRY
439
k BITS
PREVIOUS
PPO
k BITS
INCREMENTER CARRY
CARRY IN
375
ADDER (k BITS)
385
k BITS
TO R_{2p}
300'

FIG.15

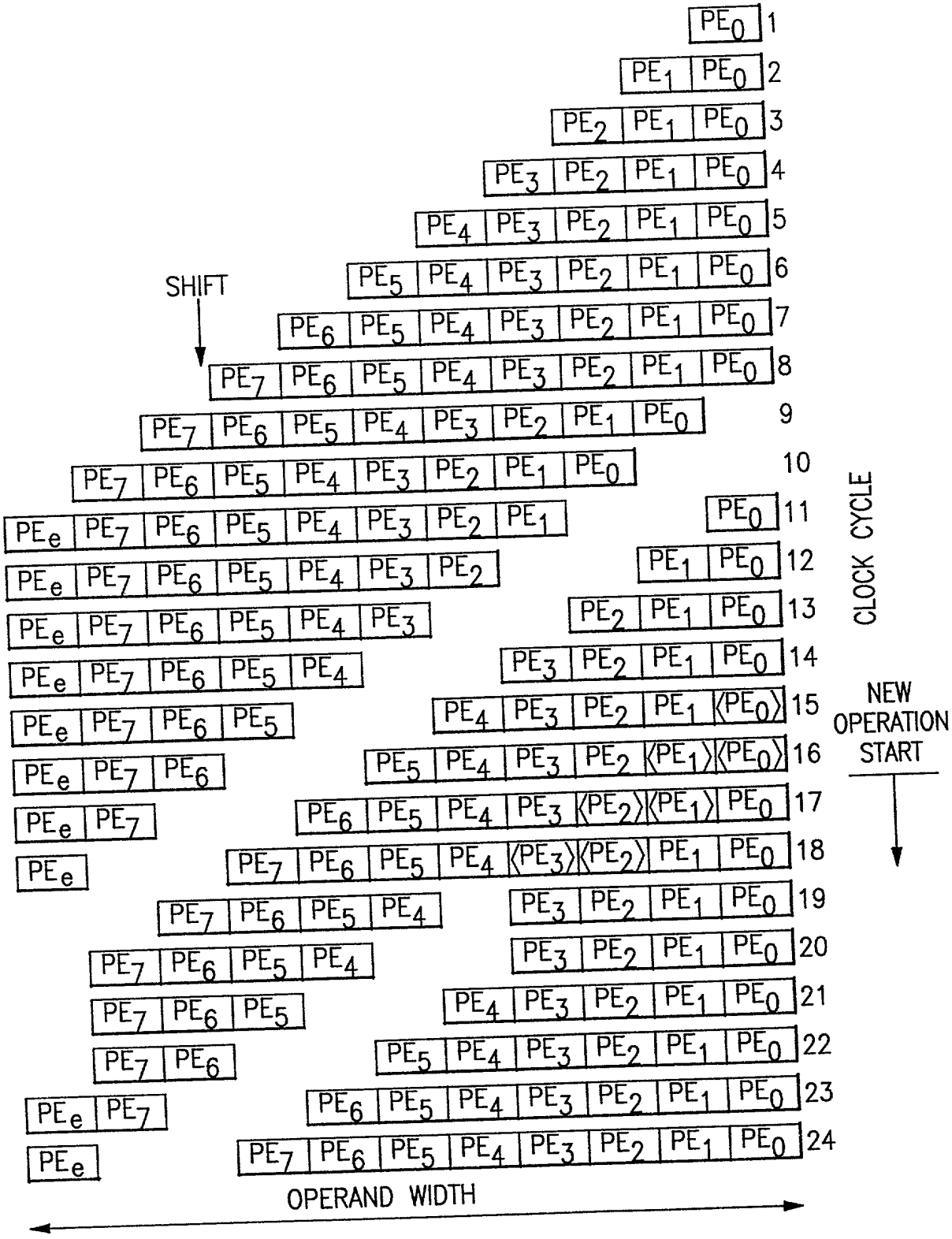

FIG.16

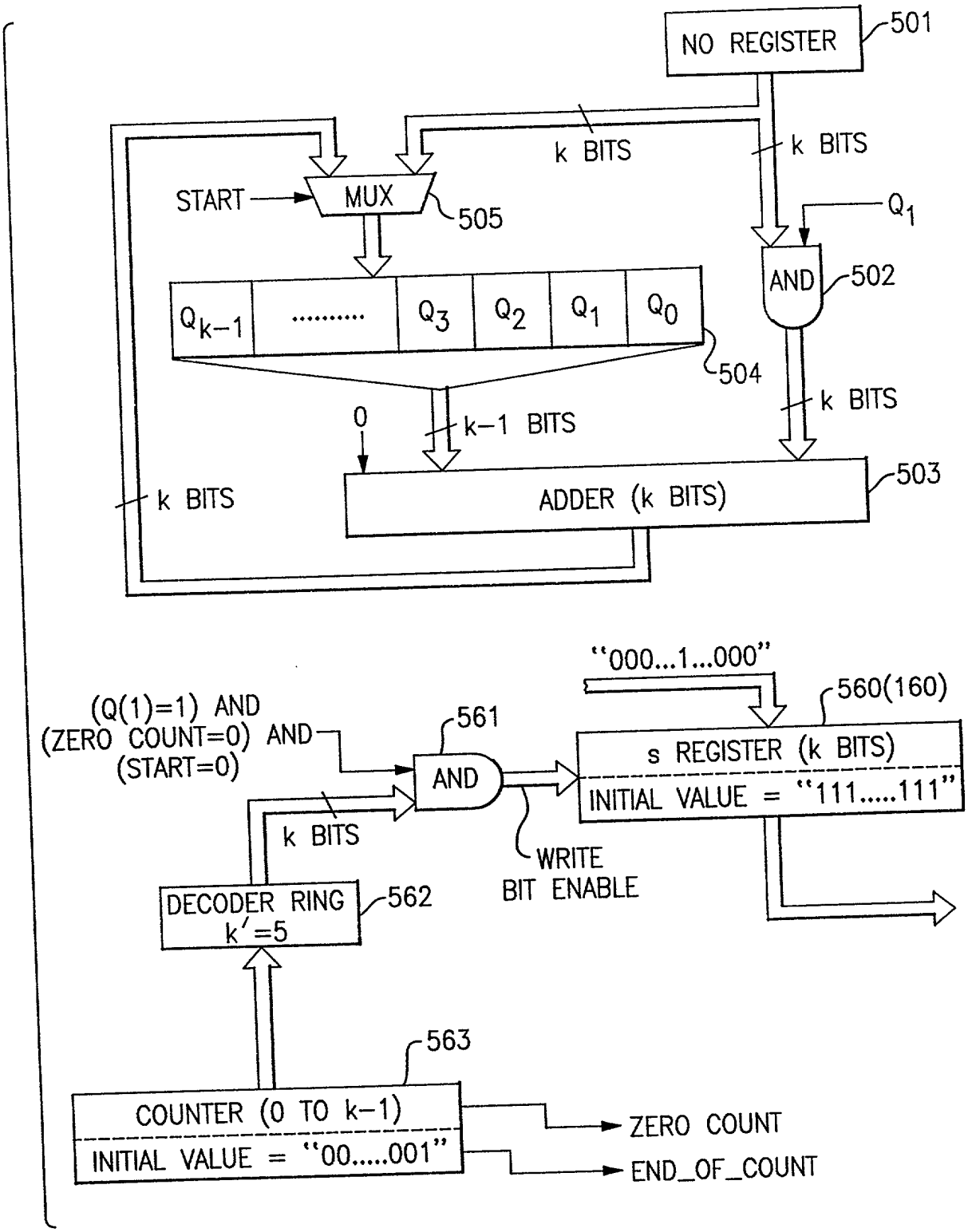
NO REGISTER
501
k BITS
k BITS
START
MUX
505
Q1
AND
502
Qk-1
.....
Q3
Q2
Q1
Q0
504
k BITS
0
k-1 BITS
k BITS
ADDER (k BITS)
503
"000...1...000"
560(160)
(Q(1)=1) AND
(ZERO COUNT=0) AND
(START=0)
561
AND
s REGISTER (k BITS)
INITIAL VALUE = "111.....111"
k BITS
WRITE
BIT ENABLE
DECODER RING
k'=5
562
563
COUNTER (0 TO k-1)
INITIAL VALUE = "00.....001"
ZERO COUNT
END_OF_COUNT

FIG.17

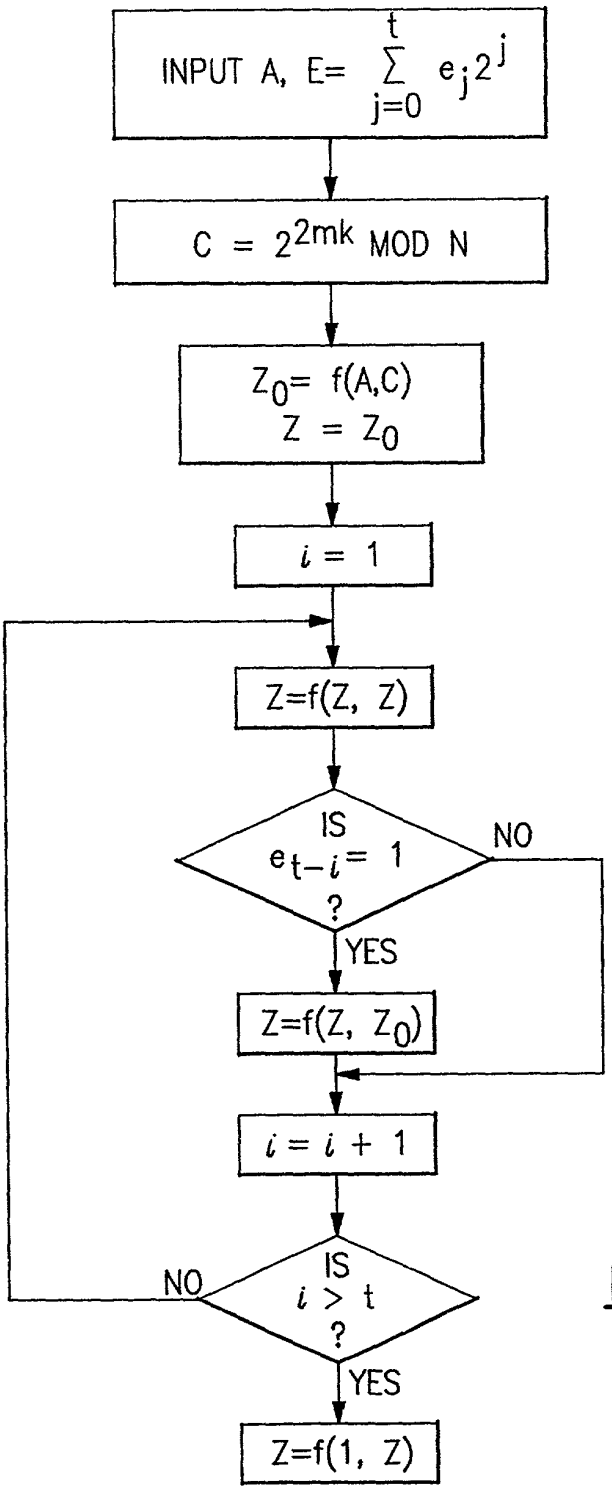
INPUT A, E= $\sum_{j=0}^{t} e_j 2^j$
C = 2^{2mk} MOD N
Z_0= f(A,C)
Z = Z_0
i = 1
Z=f(Z, Z)
IS e_{t-i}= 1 ?
NO
YES
Z=f(Z, Z_0)
i = i + 1
IS i > t ?
NO
YES
Z=f(1, Z)

FIG.18

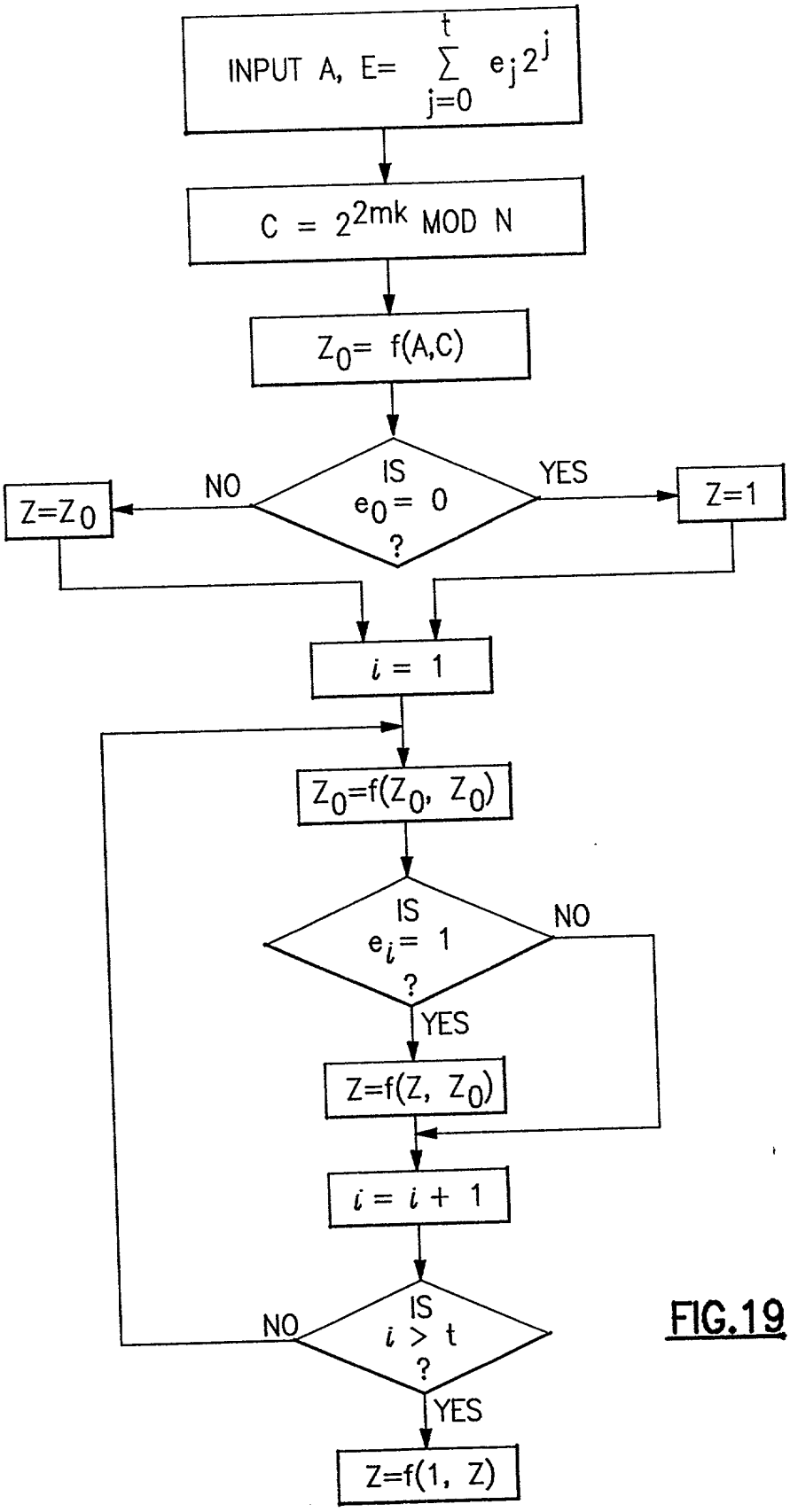
INPUT A, E= $\sum_{j=0}^{t} e_j 2^j$
C = 2^{2mk} MOD N
Z_0= f(A,C)
IS e_0= 0 ?
NO
YES
Z=Z_0
Z=1
i = 1
Z_0=f(Z_0, Z_0)
IS e_i= 1 ?
NO
YES
Z=f(Z, Z_0)
i = i + 1
IS i > t ?
NO
YES
Z=f(1, Z)

FIG.19

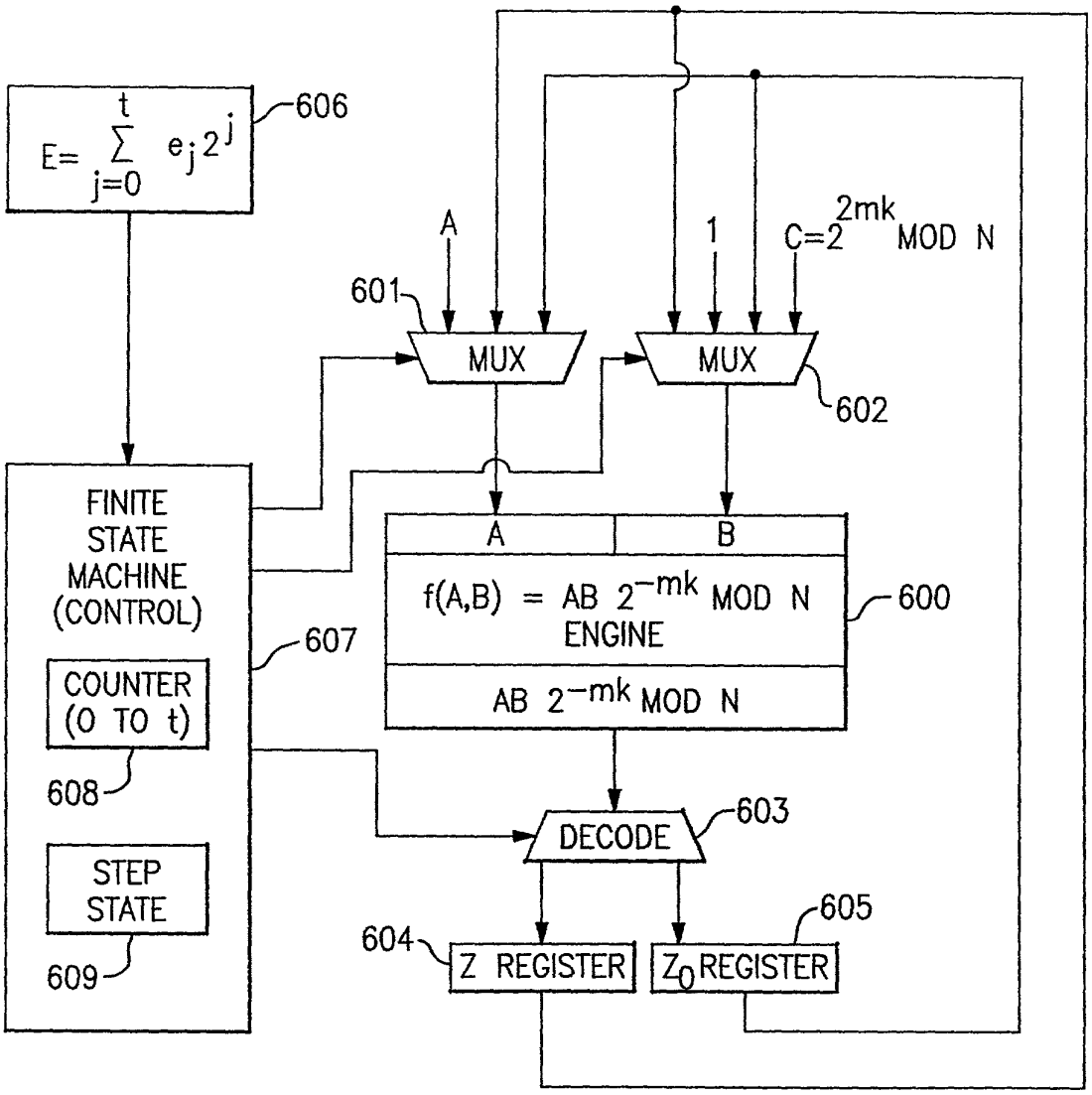
$E=\sum_{j=0}^{t} e_j 2^j$
606
A
1
$C=2^{2mk}$ MOD N
601
MUX
MUX
602
FINITE STATE MACHINE (CONTROL)
607
COUNTER (0 TO t)
608
STEP STATE
609
A
B
f(A,B) = AB 2^{-mk} MOD N ENGINE
600
AB 2^{-mk} MOD N
DECODE
603
604
Z REGISTER
Z_0 REGISTER
605

FIG.20

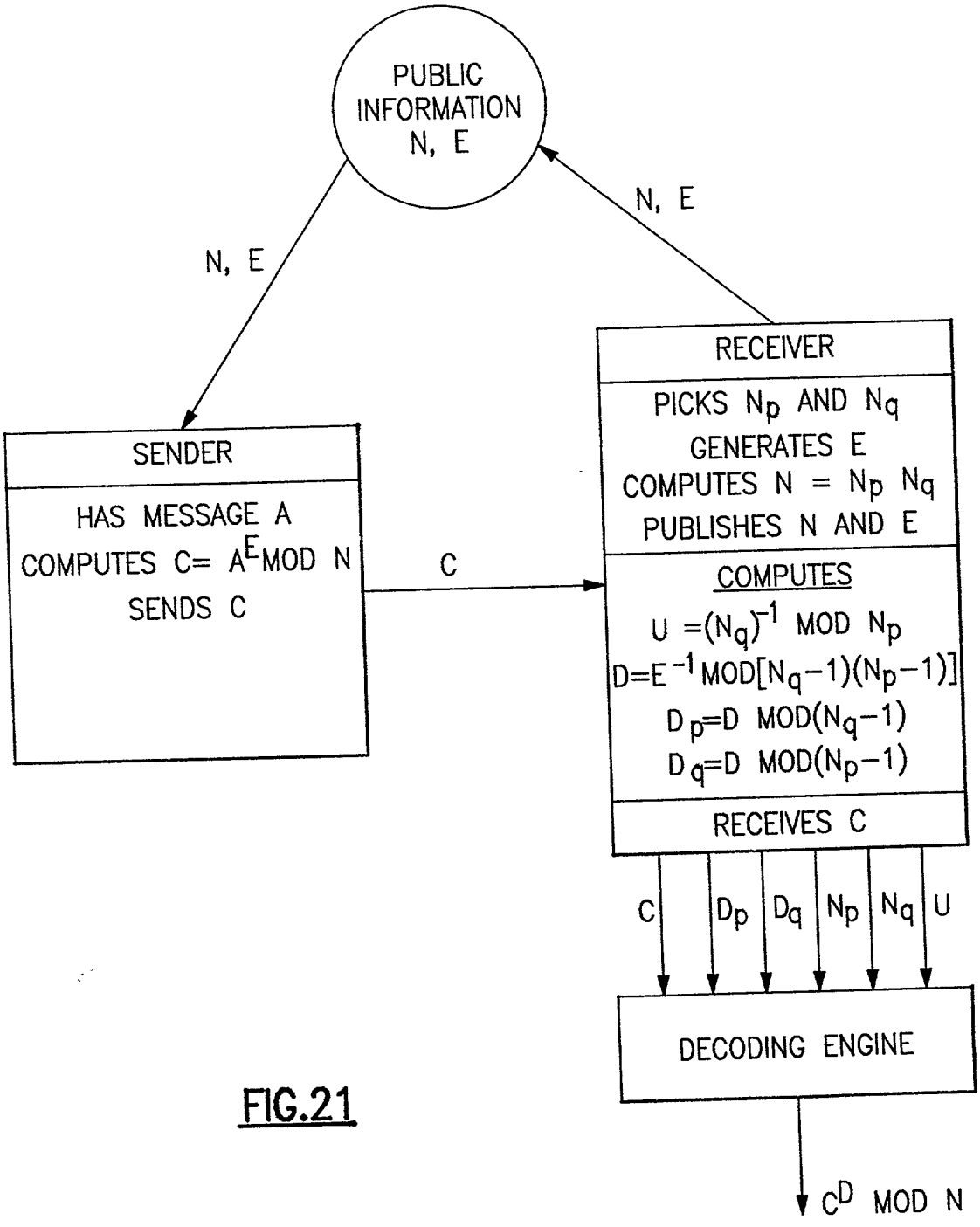
PUBLIC INFORMATION N, E
N, E
N, E
SENDER
HAS MESSAGE A
COMPUTES C= A^E MOD N
SENDS C
C
RECEIVER
PICKS Np AND Nq
GENERATES E
COMPUTES N = Np Nq
PUBLISHES N AND E
COMPUTES
U =(Nq)^-1 MOD Np
D=E^-1 MOD[Nq-1)(Np-1)]
Dp=D MOD(Nq-1)
Dq=D MOD(Np-1)
RECEIVES C
C
Dp
Dq
Np
Nq
U
DECODING ENGINE
C^D MOD N

FIG.21

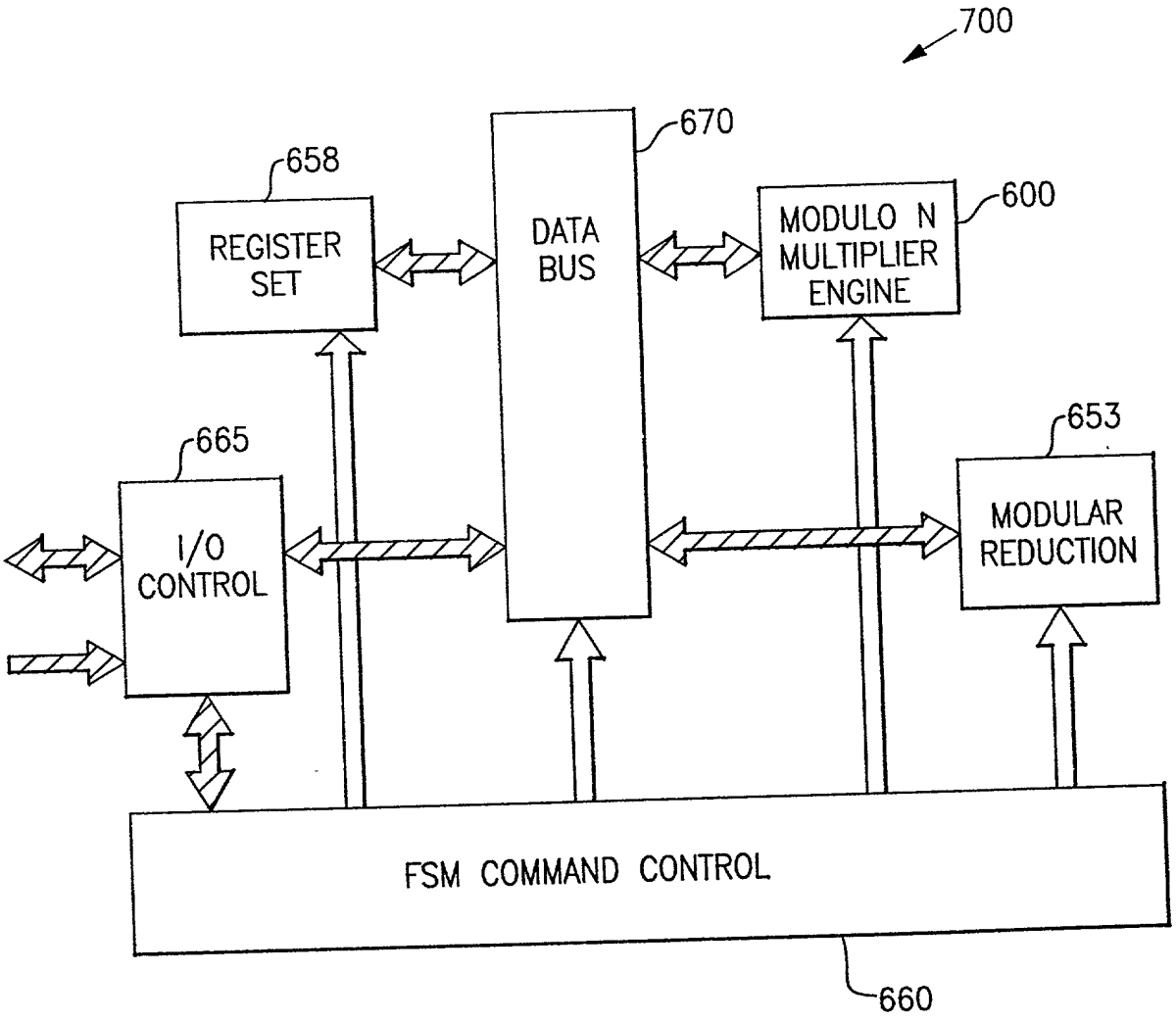
700
670
658
REGISTER SET
DATA BUS
MODULO N MULTIPLIER ENGINE
600
665
I/O CONTROL
653
MODULAR REDUCTION
FSM COMMAND CONTROL
660

FIG.22

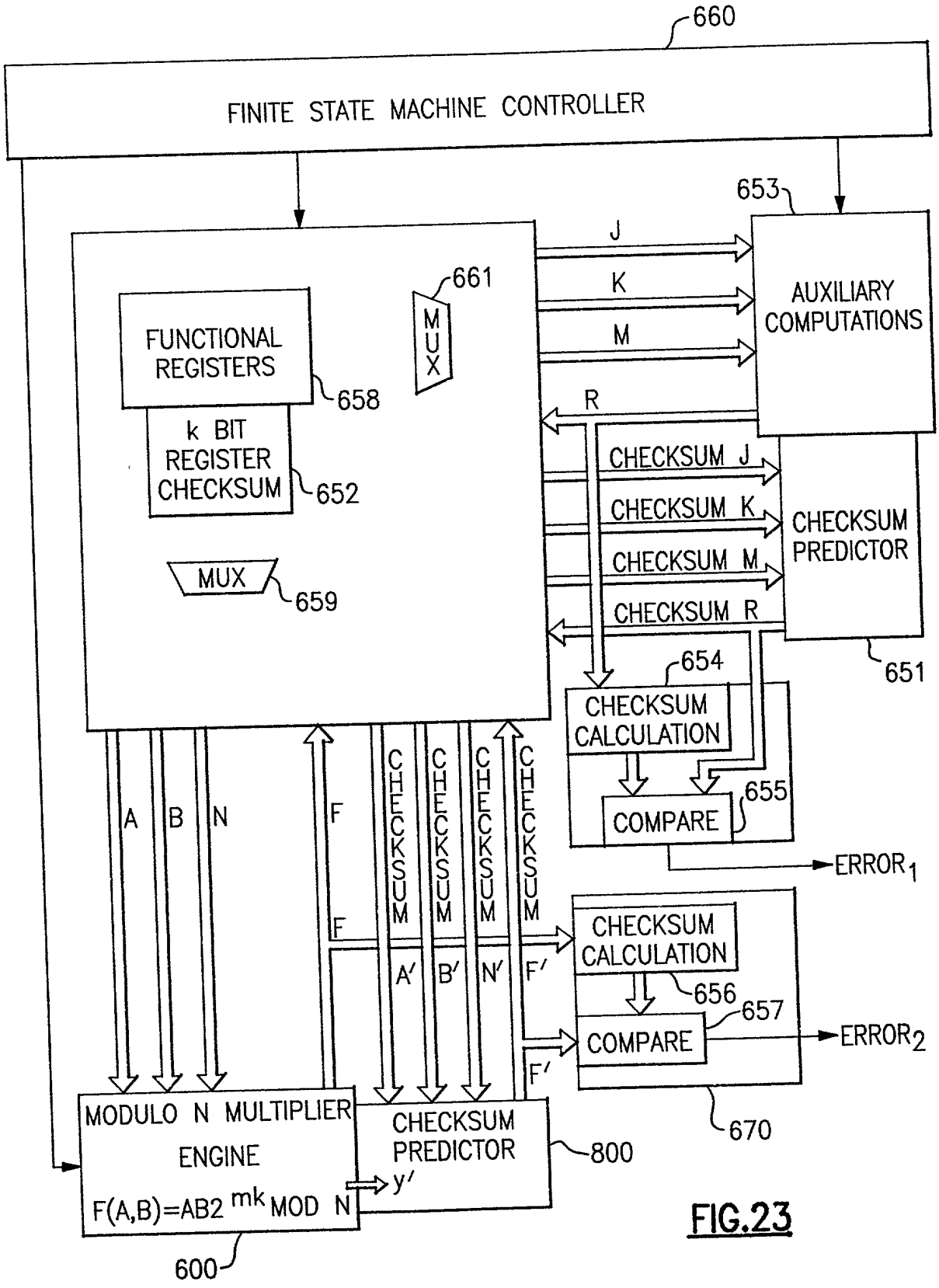
660
FINITE STATE MACHINE CONTROLLER
653
AUXILIARY COMPUTATIONS
J
K
M
R
661
MUX
FUNCTIONAL REGISTERS
658
k BIT REGISTER CHECKSUM
652
MUX
659
CHECKSUM J
CHECKSUM K
CHECKSUM M
CHECKSUM R
CHECKSUM PREDICTOR
651
654
CHECKSUM CALCULATION
655
COMPARE
ERROR1
A
B
N
F
CHECKSUM
CHECKSUM
CHECKSUM
CHECKSUM
F
A′
B′
N′
F′
CHECKSUM CALCULATION
656
657
COMPARE
ERROR2
F′
MODULO N MULTIPLIER ENGINE
F(A,B)=AB2 mk MOD N
600
CHECKSUM PREDICTOR
800
y′
670

FIG.23

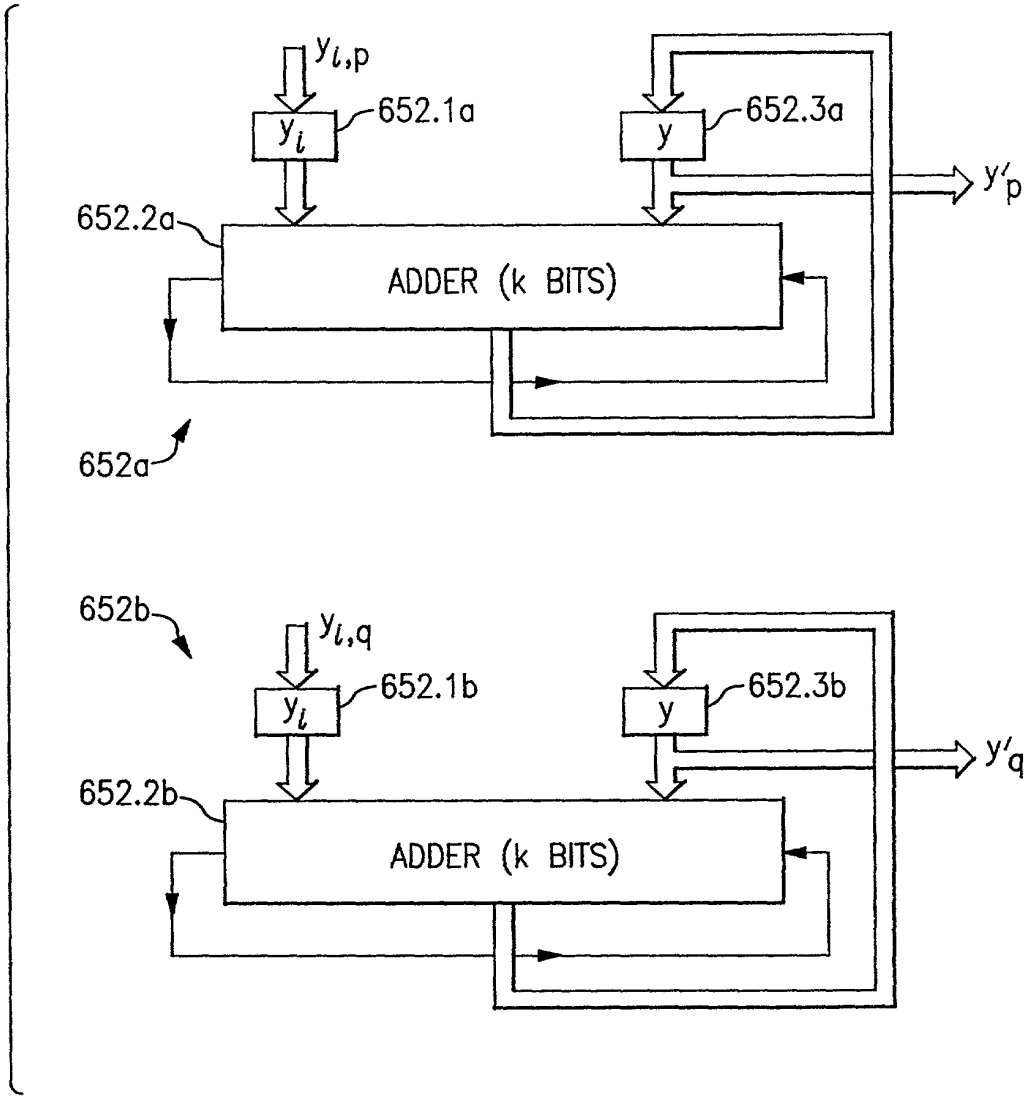
y_i,p
652.1a
y_i
y
652.3a
y'p
652.2a
ADDER (k BITS)
652a
652b
y_i,q
652.1b
y_i
y
652.3b
y'q
652.2b
ADDER (k BITS)

FIG.24

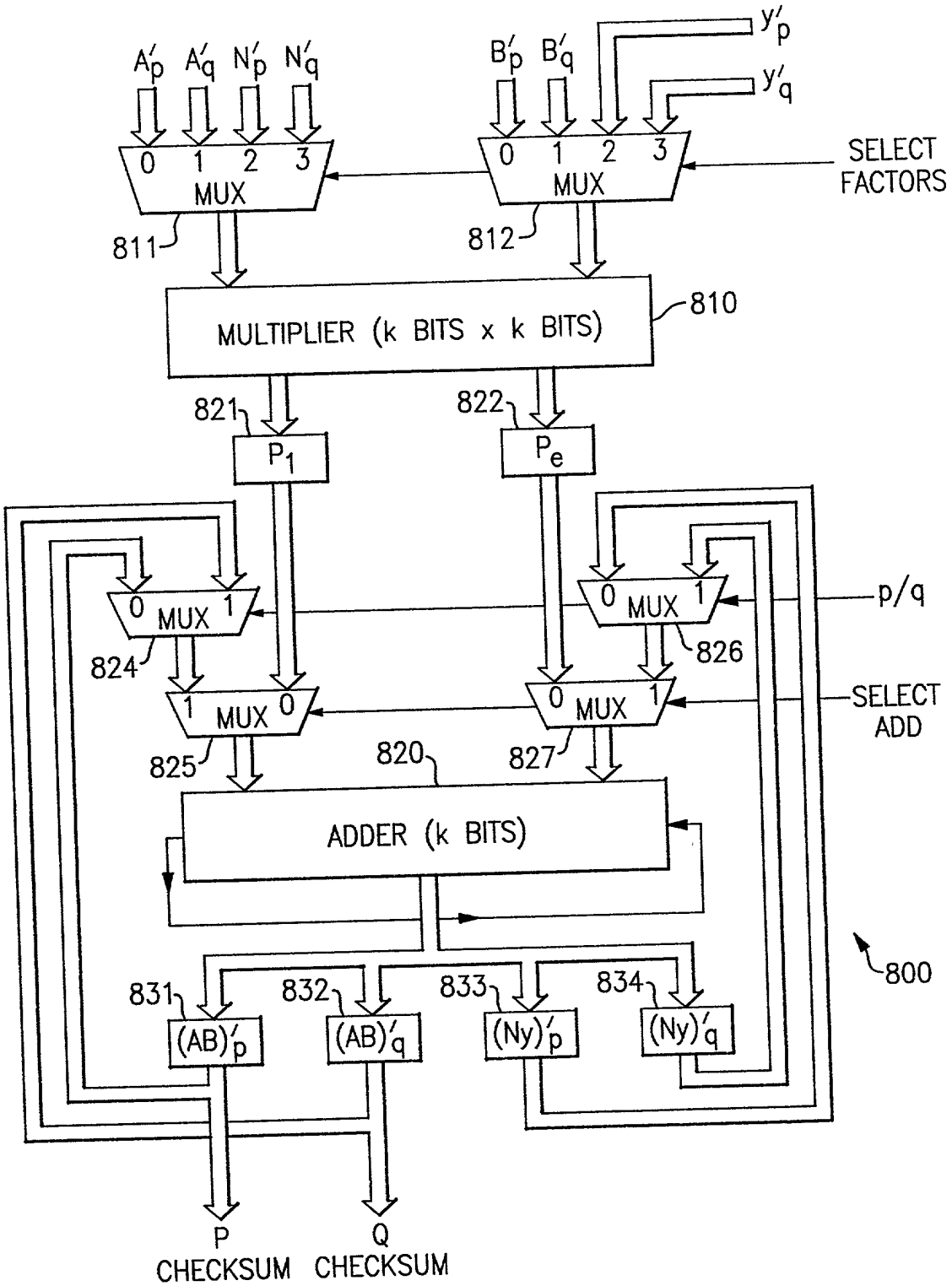
A'p A'q N'p N'q
B'p B'q
y'p
y'q
0 1 2 3
MUX
SELECT FACTORS
811
812
MULTIPLIER (k BITS x k BITS)
810
821
822
P1
Pe
p/q
824
826
SELECT ADD
825
820
827
ADDER (k BITS)
800
831
832
833
834
(AB)'p
(AB)'q
(Ny)'p
(Ny)'q
P CHECKSUM
Q CHECKSUM

FIG.25

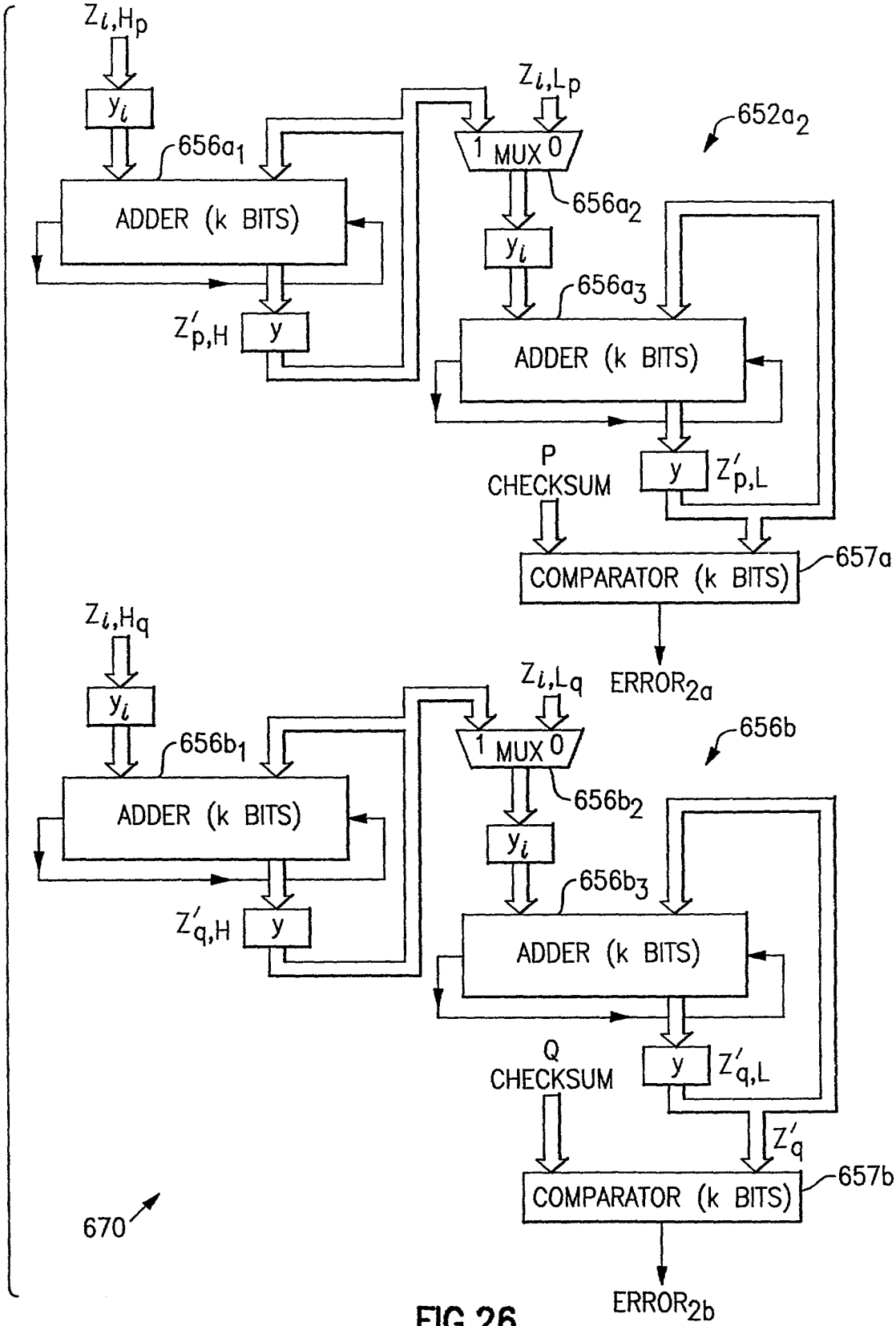
Z_i,H_p
y_i
$656a_1$
ADDER (k BITS)
$Z'_{p,H}$
y
Z_i,L_p
1 MUX 0
$652a_2$
$656a_2$
y_i
$656a_3$
ADDER (k BITS)
P CHECKSUM
y
$Z'_{p,L}$
COMPARATOR (k BITS)
657a
Z_i,H_q
y_i
$656b_1$
ADDER (k BITS)
$Z'_{q,H}$
y
Z_i,L_q
$ERROR_{2a}$
1 MUX 0
656b
$656b_2$
y_i
$656b_3$
ADDER (k BITS)
Q CHECKSUM
y
$Z'_{q,L}$
Z'_q
COMPARATOR (k BITS)
657b
670
$ERROR_{2b}$

FIG.26